FortiClient - Administration Guide

VERSION 5.2.6

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

July 22, 2016

FortiClient 5.2.6 Administration Guide

04-526-225910-20160722

TABLE OF CONTENTS

Change Log

Date	Change Description
2014-06-13	Initial release.
2014-06-27	Added a log message reference appendix.
2014-08-18	Updated for FortiClient 5.2.1.
2014-11-18	Updated for FortiClient 5.2.2.
2015-01-14	Updated for FortiClient 5.2.3.
2015-07-27	Updated for FortiClient 5.2.4.
2015-11-05	Updated for FortiClient 5.2.5.
2016-07-22	Updated for FortiClient 5.2.6.

Introduction

FortiClient provides a comprehensive network security solution for endpoints while improving your visibility and control. FortiClient allows you to manage the security of multiple endpoint devices from the FortiGate interface. This document provides an overview of FortiClient 5.2.6.

This document was written for FortiClient (Windows) 5.2.6. Not all features described in this document are supported for FortiClient (Mac OS X) 5.2.6.

FortiClient features

The following table provides a feature comparison between the standalone client (free version) and the managed client (licensed version).

Standalone Client (Free Version)	Managed Client (Licensed Version)
Installation Options • Complete: All Endpoint Security and VPN components will be installed. • VPN Only: only VPN components (IPsec and SSL) will be installed. • Create a custom FortiClient installer using the FortiClient Configurator tool using the trial mode. In trial mode, all online updates are disabled.	**Installation Options** • Complete: All Endpoint Security and VPN components will be installed. • VPN Only: only VPN components (IPsec and SSL) will be installed. • Create a custom FortiClient installer using the FortiClient Configurator tool.
Threat Protection • Real-time Antivirus Protection • Antirootkit/Antimalware • Grayware Blocking (Adware/Riskware)	**Threat Protection** • Real-time Antivirus Protection • Antirootkit/Antimalware • Grayware Blocking (Adware/Riskware) • Cloud Based Behavior Scanning
Web Content • Web Filtering • Search Engine Safe Search • Bing and Yandex • YouTube Education Filter	**Web Content** • Web Filtering • Search Engine Safe Search • Bing and Yandex • YouTube Education Filter

Standalone Client (Free Version)	Managed Client (Licensed Version)
VPN • SSL VPN • IPsec VPN • Client Certificate Support • X.509 Certificate Support • Elliptical Curve Certificate Support • Two-Factor Authentication	**VPN** • SSL VPN • IPsec VPN • Client Certificate Support • X.509 Certificate Support • Elliptical Curve Certificate Support • Two-Factor Authentication
Logging • VPN, Antivirus, Web Security, and Update Logging • View logs locally	**Logging** • VPN, Application Firewall, Antivirus, Web Filter, Update, and Vulnerability Scan Logging • View logs locally
	Application Control • Application Firewall • Block Specific Application Traffic
	Vulnerability Management • Vulnerability Scan • Link to FortiGuard with information on the impact and recommended actions
	Central Management • Centralized Client Management and monitoring • Centralized configuration provisioning and deployment • Enforcement of enterprise security policies.
	Central Logging • Upload logs to a FortiAnalyzer or FortiManager. FortiClient must be registered to FortiGate to upload logs to FortiAnalyzer or FortiManager.

Licensing

Licensing on the FortiGate is based on the number of registered clients. FortiGate 30 series and higher models support ten (10) free managed FortiClient licenses. For additional managed clients, a FortiClient license subscription must be purchased. The maximum number of managed clients varies per device model.

The VPN on-net, off-net feature in Endpoint Control will be activated only when the FortiGate, to which FortiClient is registered, is running FortiOS v5.2 with a FortiClient v5.2 license.

Client limits

The following table shows client limits per FortiGate model series.

FortiGate Series	Free Registrations	FortiClient License Upgrade
FortiGate/FortiWiFi 30 to 90 series	10	1 year FortiClient license subscription for up to 200 clients
FortiGate 100 to 300 series	10	1 year FortiClient license subscription for up to 600 clients
FortiGate 500 to 800 series, FortiGate vM01, FortiGate VM02	10	1 year FortiClient license subscription for up to 2000 clients
FortiGate 1000 series, FortiGate VM04	10	1 year FortiClient license subscription for up to 8000 clients
FortiGate 3000 to 5000 series, FortiGate VM08	10	1 year FortiClient license subscription for up to 20 000 clients

In high availability (HA) configurations, all cluster members require an upgrade license key.

For more information, go to www.forticlient.com.

The FortiClient license for FortiOS version 5.2 includes the license file required to use the FortiClient Configurator tool used to create custom FortiClient installers. The Configurator tool also allows you to rebrand the installer file.

Installation information

The following table lists operating system support and the minimum system requirements.

Operating System Support	Minimum System Requirements
• Microsoft Windows XP (32-bit) • Microsoft Windows Vista (32-bit and 64-bit) • Microsoft Windows 7 (32-bit and 64-bit) • Microsoft Windows 8 (32-bit and 64-bit) • Microsoft Windows 8.1 (32-bit and 64-bit)	• Microsoft Internet Explorer version 8 or later • Microsoft Windows compatible computer with Intel processor or equivalent • Compatible operating system and minimum 512MB RAM • 600MB free hard disk space • Native Microsoft TCP/IP communication protocol • Native Microsoft PPP dialer for dial-up connections • Ethernet NIC for network connections • Wireless adapter for wireless network connections • Adobe Acrobat Reader for documentation • MSI installer 3.0 or later.
• Microsoft Windows Server 2008 R2 • Microsoft Windows Server 2012	• Microsoft Internet Explorer version 8 or later • Microsoft Windows compatible computer with Intel processor or equivalent • Compatible operating system and minimum 512MB RAM • 600MB free hard disk space • Native Microsoft TCP/IP communication protocol • Native Microsoft PPP dialer for dial-up connections • Ethernet NIC for network connections • Wireless adapter for wireless network connections • Adobe Acrobat Reader for documentation • MSI installer 3.0 or later.
• Mac OS X v10.8 Mountain Lion • Mac OS X v10.9 Mavericks • Mac OS X v10.10 Yosemite	• Apple Mac computer with an Intel processor • 256MB of RAM • 20MB of hard disk drive (HDD) space • TCP/IP communication protocol • Ethernet NIC for network connections • Wireless adapter for wireless network connections

Firmware images and tools

Microsoft Windows

The following files are available in the firmware image file folder:

- FortiClientSetup_5.2.xx.xxxx.exe
  Standard installer for Microsoft Windows (32-bit).

- FortiClientSetup_5.2.xx.xxxx.zip
  A zip package containing FortiClient.msi and language transforms for Microsoft Windows (32-bit). Some properties of the MSI package can be customized with FortiClient Configurator tool.
- FortiClientSetup_5.2.xx.xxxx_x64.exe
  Standard installer for Microsoft Windows (64-bit).
- FortiClientSetup_5.2.xx.xxxx_x64.zip
  A zip package containing FortiClient.msi and language transforms for Microsoft Windows (64-bit). Some properties of the MSI package can be customized with FortiClient Configurator tool.
- FortiClientTools_5.2.xx.xxxx.zip
  A zip package containing miscellaneous tools including the FortiClient Configurator tool and VPN Automation files.

When creating a custom FortiClient v5.2 installer using the FortiClient Configurator tool, you can choose to which features to install. You can also select to enable or disable software updates, configure SSO, and rebrand FortiClient

Mac OS X

The following files are available in the firmware image file folder:

- FortiClient_5.2.x.xxx_macosx.dmg
  Standard installer or Mac OS X.
- FortiClientTools_5.2.x.xxx_macosx.tar
  FortiClient includes various utility tools and files to help with installations. The following tools and files are available in the FortiClientTools `.tar` file:
- OnlineInstaller
  This file downloads and installs the latest FortiClient file from the public FDS.
- FortiClientConfigurator
  An installer repackaging tool that is used to create customized installation packages.
- RebrandingResources
  Rebranding resources used by the FortiClient Configurator tool.

When creating a custom FortiClient 5.2.6 installer using the FortiClient Repackager tool, you can choose to install Everything, VPN Only, or SSO only. You can also select to enable or disable software updates and rebrand FortiClient.

FortiClient version 5.2 cannot use FortiClient version 5.0 licenses. To use FortiClient Configurator, you need to use the FortiClient version 5.2 license file.

Language support

The following table lists FortiClient language support information.

Language	Graphical User Interface	XML Configuration	Documentation
English (United States)	✓	✓	✓
Chinese (Simplified)	✓	-	-
Chinese (Traditional)	✓	-	-
French (France)	✓	-	-
German	✓	-	-
Japanese	✓	-	-
Korean	✓	-	-
Portuguese (Brazil)	✓	-	-
Spanish (Spain)	✓	-	-

Please review the *FortiClient (Windows) Release Notes* or the *FortiClient (Mac OS X) Release Notes* prior to upgrading. Release Notes are available at the Customer Service & Support portal.

FortiClient language is dependent on the regional settings on the client workstation. When the regional language setting is not supported, FortiClient defaults to English.

What's New in FortiClient 5.2

The following is a list of new features and enhancements in FortiClient version 5.2.

This document was written for FortiClient (Windows) 5.2.6. Not all features described in this document are supported for FortiClient (Mac OS X) 5.2.6.

New features in FortiClient 5.2.6

There are no new features in FortiClient version 5.2.6.

New features in FortiClient 5.2.5

There are no new features in FortiClient version 5.2.5.

New features in FortiClient 5.2.4

The following is a list of new features in FortiClient version 5.2.4.

SSL VPN connections on a Mac OS X computer

When FortiClient is configured with an SSL VPN connection on a Mac OS X computer, a certificate warning message is now displayed when the certification subject name does not match the destination host name of the SSL server. A server certificate is invalid if:

- It has expired
- It cannot be verified with a certificate authority
- The server name does not match the name in the certificate

New features in FortiClient 5.2.3

The following is a list of new features in FortiClient version 5.2.3.

Log upload to Syslog server

FortiClient may be configured to send log messages to a syslog server. The following XML configuration may be used to enable this feature:

```
<forticlient_configuration>
   <system>
      <log_settings>
```

```
            <remote_logging>
               <log_protocol>syslog</log_protocol> <!-- faz | syslog -->
               <netlog_server></netlog_server> <!-- server IP address -->
            </remote_logging>
         </log_settings>
      </system>
   </forticlient_configuration>
```

Set `<log_protocol>` to `faz` in order to switch logging to FortiAnalyzer. This is the default. Provide the IP address of the syslog server in `<netlog_server>`.

OpenSSL library

The OpenSSL library has been updated to the latest version 1.0.1k.

New features in FortiClient 5.2.2

The following is a list of new features in FortiClient version 5.2.2.

Certificates

Elliptical curve certificates are now supported for both IPsec and SSL VPN.

OpenSSL library

The OpenSSL library has been updated to the latest version 1.0.1j.

New features in FortiClient 5.2.1

The following is a list of new features in FortiClient 5.2.1

OpenSSL library

The OpenSSL library has been updated to the latest version 1.0.1i.

Logging to FortiManager/FortiAnalyzer

Uploading logs to FortiManager or FortiAnalyzer requires FortiClient to be registered to a FortiGate.

New features in FortiClient 5.2.0

The following is a list of new features in FortiClient version 5.2.0.

Antivirus

Malware cleanup in safe mode

Malware that is already on a Microsoft Windows computer system that could not be removed in normal mode, may be removed by running FortiClient in safe mode. Only the FortiClient Antivirus feature is available in safe mode. Full or custom antivirus scans can be started from while in safe mode. The resulting log files and any quarantined files, will be available both in safe mode, as well as after returning to normal mode.

The FortiClient installer always runs a quick antivirus scan on the target host system before proceeding with the installation. In case a virus on an infected system prevents downloading of the new FortiClient package, you can boot into safe mode, run the FortiClient installer to scan and quarantine the virus or malware, and then proceed with the installation.

Protection against security threats in URLs has moved to the Antivirus module

Malicious and Phishing URLs were previously configured and blocked as part of the Web Filtering feature. These are in the Security Risk category. This category has now been moved to become part of the Antivirus feature. When a custom FortiClient installation is created without the antivirus module, these threats are blocked by the Web Filtering feature.

View real-time protection events in the console

When an antivirus real-time protection event has occurred you can select to view these events in the FortiClient console. Select *AntiVirus* > *Threats Detected* and select *Real-time Protection events*. The `realtime_scan.log` will open in the default viewer.

Example log output:

```
Realtime scan result:
time: 03/18/14 10:46:07, virus found: EICAR_TEST_FILE, action: Quarantined,
    c:\users\user\desktop\eicar.com
time: 03/18/14 10:46:07, virus found: EICAR_TEST_FILE, action: Quarantined,
    c:\users\user\desktop\eicar.com.txt
time: 03/18/14 10:46:07, virus found: EICAR_TEST_FILE, action: Quarantined,
    c:\users\user\desktop\eicarcom2.zip
time: 03/18/14 10:46:08, virus found: EICAR_TEST_FILE, action: Quarantined,
    c:\users\user\desktop\eicar_com.zip
time: 03/18/14 10:46:39, virus found: EICAR_TEST_FILE, action: Quarantined,
    c:\users\user\appdata\local\temp\3g_bl8y9.com.part
time: 03/18/14 10:48:13, virus found: EICAR_TEST_FILE, action: Quarantined,
    c:\users\user\appdata\local\temp\xntwh8q1.zip.part
```

Removable media scan

In FortiClient v5.2 you can select to perform an antivirus scan of all connected devices with removable storage. Select *AntiVirus* > *Scan Now* > *Removable media Scan* to scan these connected devices. When performing a *Full Scan*, removable storage is also scanned.

One-click button to enable antivirus

In the FortiClient console, you can enable the antivirus feature using a single button visible in the header. This is convenient in the event that you are on a tab other than the Antivirus tab. The button is visible only when Real-time Protection is disabled.

Web Filtering

Manual URL filter list support

FortiClient now supports URL filters configured in the FortiOS security profile and applied to the FortiClient Profile.

Web Security

FortiClient Parental Control has been renamed Web Security. When FortiClient is registered to a FortiGate, Web Security is named Web Filter.

VPN

VPN over IPv6

VPN connections to the FortiGate can be established on a network that is configured with IPv6. New connections may be configured from the FortiClient console or through the XML configuration file. IPv6 is supported for IPsec and SSL VPN.

Note that FortiOS only supports VPN over IPv6 when both sides of the connection are using IPv6. A network with one end using IPv6 while the other end uses IPv4 is not supported.

Advanced VPN configuration in the FortiClient console

VPN configurations through the FortiClient console have been simplified since FortiClient v5.0. Only a few configuration entries were required and advanced configuration required use of the XML configuration file. In FortiClient v5.2 you can access IPsec VPN advanced settings in the FortiClient console. These advanced settings are useful when setting up connections to an IPsec VPN server other than a FortiGate.

Simplified FortiClient console for VPN only installations

FortiClient features may be customized in one of three ways:

- In the standard FortiClient installer,
- In the FortiClient Configurator tool,
- In the FortiGate FortiClient Profile, you can turn off and hide unused features.

When only the VPN feature is selected with any of these three methods, FortiClient will present a simplified console, with no tabs on the left-hand side.

VPN auto-connect based on DHCP off-net determination

VPN auto-connect ensures that FortiClient creates a VPN connection to the FortiGate when considered to be off-net. A site administrator, who has configured Endpoint Control on their FortiGate, may choose to enable VPN auto-connect in the Endpoint Control profile.

Computer endpoints or clients in the network should use the designated DHCP server for IP address assignments. The DHCP server sends a special tag within the protocol to identify if the client is on-net or off-net. The on-net status indicates that the endpoint is within the corporate network protected by the FortiGate.

When the client is off-net, FortiClient will automatically attempt to establish a VPN connection to the VPN server indicated in the FortiGate Endpoint Control configuration. When the client is on-net, no VPN connection is required.

This feature requires FortiOS v5.2.0 or later. The FortiGate must use a FortiClient v5.2 license.

VPN auto-connect improvements

VPN auto-connect/always-up regardless of how the VPN connection ended.

Application Firewall

Updated Application Firewall Engine

FortiClient now uses a common Application Firewall detection engine with FortiOS. This provides enhanced detection coverage. Signatures configured in the FortiGate security profile are available to FortiClient.

When the application being blocked is web-based, a message is displayed to the user in the web browser. For non-browser applications, a system tray notification is displayed. Notifications are disabled by default to reduce distractions to every day use of the system.

Endpoint Control

Improvements to the Endpoint Control page

The FortiGate *Endpoint Protection* > *FortiClient Profiles* page has been simplified.

VPN auto-connect based on DHCP off-net determination

See VPN auto-connect based on DHCP off-net determination on page 18.

Enable Vulnerability Scan module

In FortiOS v5.2, the Vulnerability Scan module is enabled via the FortiGate Command Line Interface (CLI). This feature is not available in the FortiClient Profile in the GUI until enabled via the CLI. This feature is available in FortiClient when registered to FortiGate for endpoint control.

To enable Vulnerability Scan, enter the following CLI commands:

```
config endpoint-control profile
   edit <profile-name>
      config forticlient-winmac-settings
         set forticlient-vuln-scan {enable | disable}
         set forticlient-vuln-scan-schedule {daily | weekly | monthly}
         set forticlient-vuln-scan-on-registration {enable | disable}
         set forticlient-ui-options {av | wf | af | vpn | vs}
      end
```

```
end
```

When setting the `forticlient-ui-options`, you must include all the modules that you want to enable in the FortiClient console.

Installation

Standard installation options

When installing FortiClient (Windows/Mac OS X) v5.2, you can choose the setup type that best suits your needs. Select one of the following options:

- Complete: All Endpoint Security and VPN components will be installed
- VPN Only: Only VPN components (IPsec and SSL) will be installed.

Custom install - select features to include in the FortiClient install

The FortiClient Configurator tool can be used to create custom FortiClient MSI installers with various combinations. Some of the customization options available include:

- Select FortiClient features of interest
- Provide a custom XML configuration file
- Rebrand the FortiClient product

The customized executable installer generated may be used to install on all supported platforms manually. An MSI installer is also created for distribution using Active Directory or SCCM.

A FortiClient v5.2 license is required to use the FortiClient Configurator tool.

MSI installers are support in Microsoft Windows environments only.

Client installer and Configurator updates (more granular installation options)

Select to install the complete feature set or VPN only in the regular client installer. When selecting to use the repackager, you can install the complete feature set, VPN only, or SSO only.

Client rebranding capabilities (via the Configurator tool)

You can edit various text and graphical UI elements using the rebranding option in the FortiClient Configurator tool.

Provisioning FortiClient

FortiClient can be installed on a standalone computer using the installation wizard or deployed to multiple Microsoft Windows systems using Microsoft Active Directory (AD) or the Microsoft System Center 2012 Configuration Manager (SCCM).

This chapter contains the following sections:

For information on customizing your FortiClient installation, see Custom FortiClient Installations on page 138.

Standard FortiClient installation

The following section describes installing FortiClient to a standalone Microsoft Windows and Apple Mac computer.

Download the FortiClient installation files

The FortiClient installation files can be downloaded from the following sites:

- Fortinet Customer Service & Support: https://support.fortinet.com

Requires a support account with a valid support contract. Download either the Microsoft Windows (32-bit/64-bit) or the Mac OS X online installation file.

- FortiClient homepage: www.forticlient.com

Download the FortiClient online installation file. The installer file performs a virus and malware scan of the target system prior to installing FortiClient.

- Fortinet Resource Center: http://www.fortinet.com/resource_center/product_downloads.html

Download the FortiClient online installation file. On this page you can download the latest version of FortiClient for Microsoft Windows, Mac OS X, iOS, and Android.

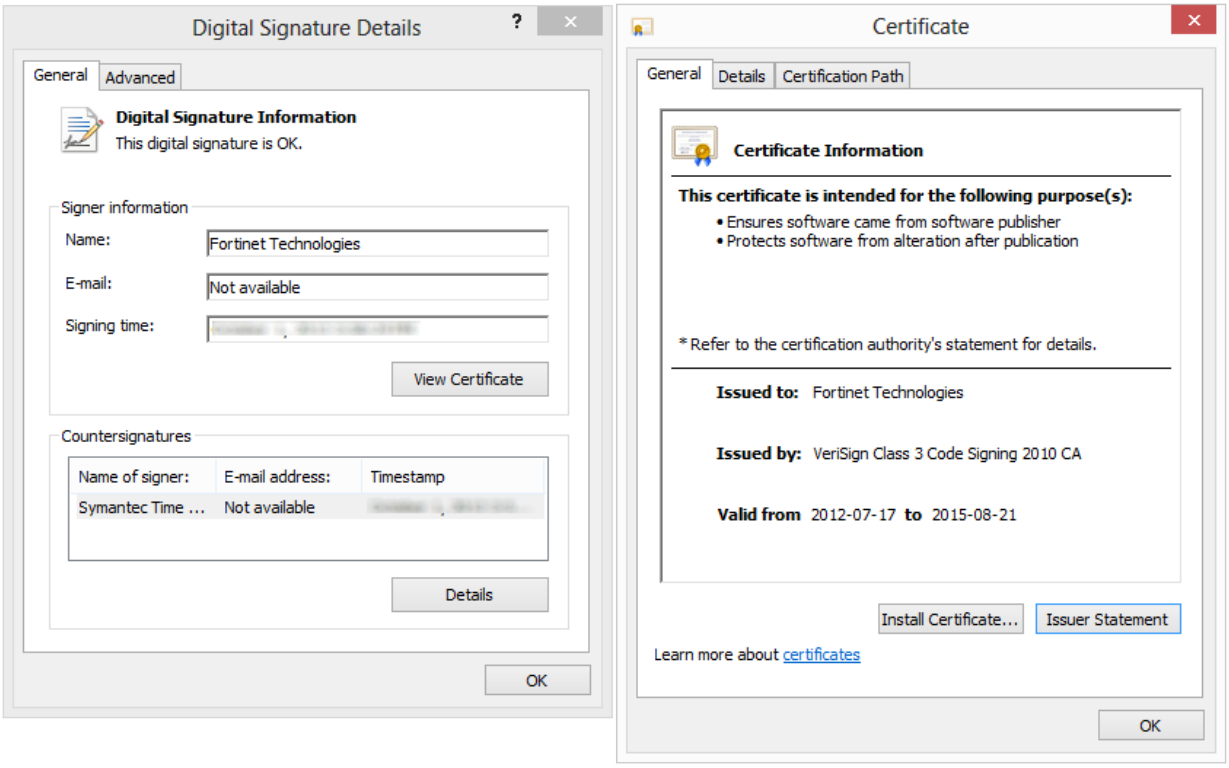
In FortiOS v5.0.1 and later, you can download the FortiClient installation files in the FortiGate dashboard. Go to *System* > *Dashboard* > *Status,* in the *License Information* widget, select *Mac* or *Windows* to download the FortiClient Online Installer file.

Install FortiClient on a Microsoft Windows computer

The following instructions will guide you though the installation of FortiClient on a Microsoft Windows computer. For more information, see the *FortiClient (Windows) Release Notes*.

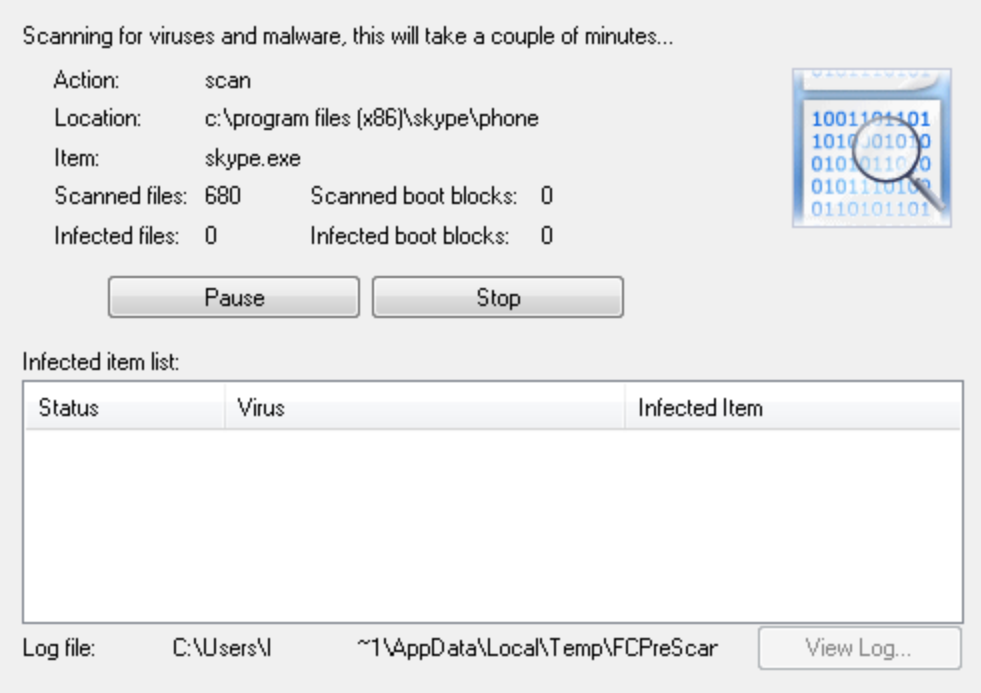
When installing FortiClient, it is recommended to use the FortiClientOnlineInstaller file. This file will launch the FortiClient Virus Cleaner which will scan the target system prior to installing the FortiClient application.

To check the digital signature of FortiClient, right-click on the installation file and select *Properties*. In this menu you can set file attributes, run the compatibility troubleshooter, view the digital signature and certificate, install the certificate, set file permissions, and view file details.



To install FortiClient (Windows):

1. Double-click the FortiClient executable file to launch the setup wizard. The *Setup Wizard* will launch on your computer. When using the FortiClient OnlineInstaller file, the FortiClient Virus Cleaner will run before launching the *Setup Wizard*. If a virus is found that prevents the infected system from downloading the new FortiClient package, see Install FortiClient on an infected system on page 25.



The *Welcome* screen is displayed.

2. Read the license agreement, select the checkbox, and select *Next* to continue. You have the option to print the EULA in this *License Agreement* screen. The *Choose Setup Type* screen is displayed.
3. Select one of the following setup types:
   - Complete: All Endpoint Security and VPN components will be installed.
   - VPN Only: Only VPN components (IPsec and SSL) will be installed.
4. Select *Next* to continue. The *Destination Folder* screen is displayed.
5. Select *Change* to choose an alternate folder destination for installation.
6. Select *Next* to continue.

   FortiClient will search the target system for other installed antivirus software. If found, FortiClient will display the *Conflicting Antivirus Software* page. You can either exit the current installation and uninstall the antivirus software, disable the antivirus feature of the conflicting software, or continue with the installation with FortiClient real-time protection disabled.

This dialog box is displayed during a new installation of FortiClient and when upgrading from an older version of FortiClient which does not have the antivirus feature installed.

It is recommended to uninstall the conflicting antivirus software before installing FortiClient or enabling the antivirus real-time protection feature. Alternatively, you can disable the antivirus feature of the conflicting software.

7. Select *Next* to continue.
8. Select *Install* to begin the installation.
9. Select *Finish* to exit the FortiClient Setup Wizard.

On a new FortiClient installation, you do not need to reboot your system. When upgrading the FortiClient version, you must restart your system for the configuration changes made to FortiClient to take effect. Select *Yes* to restart your system now, or select *No* to manually restart later.

FortiClient will update signatures and components from the FortiGuard Distribution Network (FDN).

10. If the FortiGate on the network is broadcasting discovery messages, FortiClient will attempt to register to the FortiGate.

    If the FortiGate is not broadcasting discovery messages, select the *Register to FortiGate* button in the FortiClient header, specify the address of the FortiGate in the text field, and select the *Go* icon.

If you have any questions about registering FortiClient to FortiGate, please contact your network administrator.

11. To launch FortiClient, double-click the desktop shortcut icon.

Install FortiClient on a Microsoft Server

In FortiClient v5.2 you can install FortiClient on a Microsoft Windows Server 2008 R2 or 2012 server. You can use the regular FortiClient Windows image for Server installations.

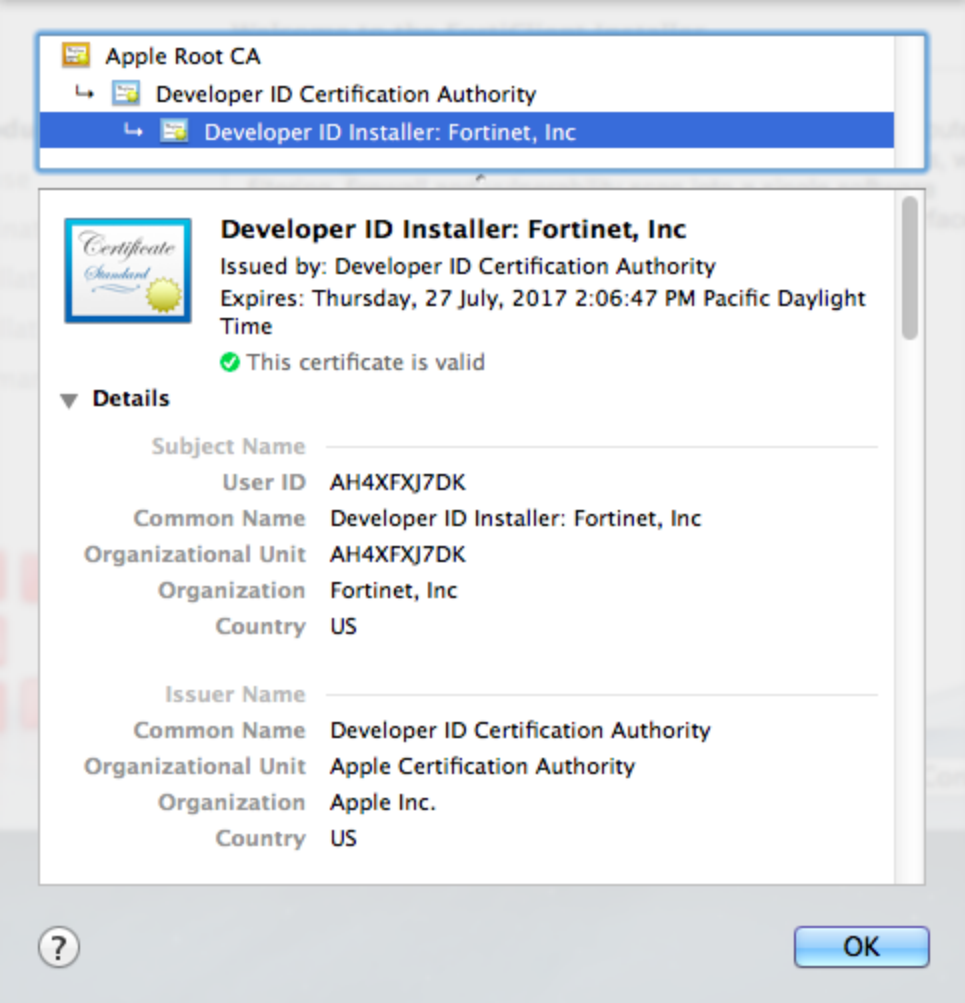
Please refer to the Microsoft knowledge base for caveats on installing antivirus software in a server environment.

Install FortiClient on a Mac OS X computer

The following instructions will guide you though the installation of FortiClient on a Mac OS X computer. For more information, see the *FortiClient (Mac OS X) 5.2.6 Release Notes*.

To install FortiClient (Mac OS X):

1. Double-click the FortiClient `.dmg` installer file to launch the FortiClient installer. The *FortiClient Installer* will install FortiClient on your computer. Select *Continue*.
2. Select the lock icon in the upper right corner to view certificate details.



3. Read the Software License Agreement and select *Continue*. You have the option to print or save the Software Agreement in this window. You will be prompted to *Agree* with the terms of the license agreement.
4. Select the destination folder for the installation.
5. Select *Install* to perform a standard installation on this computer. You can change the install location from this screen.
6. Depending on your system, you may be prompted to enter your system password.
7. The installation was successful. Select *Close* to exit the installer.
8. FortiClient has been saved to the *Applications* folder.
9. Double-click the FortiClient icon to launch the application. The application console loads to your desktop. Select the lock icon in the FortiClient console to make changes to the FortiClient configuration.

Install FortiClient on an infected system

The FortiClient installer always runs a quick antivirus scan on the target host system before proceeding with the complete installation. If the system is clean, installation proceeds as usual.

Any virus found during this step is quarantined before installation continues.

In case a virus on an infected system prevents downloading of the new FortiClient package, use the following process:

- Boot into “safe mode with networking” (which is required for the FortiClient installer to download the latest signature packages from the Fortinet Distribution Network).
- Run the FortiClient installer.

This scans the entire file system. A log file is generated in the logs subdirectory. If a virus is found, it will be quarantined. When complete, reboot back into normal mode and run the FortiClient installer to complete the installation.

Microsoft Windows will not allow FortiClient installation to complete in safe mode. An error message will be generated. It is necessary to reboot back into normal mode to complete the installation.

Install FortiClient as part of a cloned disk image

If you configure computers using a cloned hard disk image, you need to remove the unique identifier from the FortiClient application. You will encounter problems with FortiGate if you deploy multiple FortiClient applications with the same identifier.

This section describes how to include a custom FortiClient installation in a cloned hard disk image but remove its unique identifier. On each computer configured with the cloned hard disk image, the FortiClient application will generate its own unique identifier the first time the computer is started.

To include a FortiClient installation in a hard disk image:

1. Using an MSI FortiClient installer, install and configure the FortiClient application to suit your requirements. You can use a standard or a customized installation package.
2. Right-click the FortiClient icon in the system tray and select Shutdown FortiClient.
3. From the folder where you expanded the FortiClientTools.zip file, run RemoveFCTID.exe. The RemoveFCTID tool requires administrative rights.

Do not include the RemoveFCTID tool as part of a logon script.

4. Shut down the computer.

Do not reboot the Windows operating system on the computer before you create the hard disk image. The FortiClient identifier is created before you log on.

5. Create the hard disk image and deploy it as needed.

Install FortiClient on cloned computers

If you intend to create an image of the hard drive for deployment to other computers, you need to shut down FortiClient and use the RemoveFCTID tool to remove the FortiClient identifier. For more information, see Install

FortiClient as part of a cloned disk image on page 26.

Deploy FortiClient using Microsoft Active Directory (AD) server

There are multiple ways to deploy FortiClient to endpoint devices including using Microsoft Active Directory.

The following instructions are based from Microsoft Windows Server 2008. If you are using a different version of Microsoft Server, your MMC or snap-in locations may be different.

Using Microsoft AD to deploy FortiClient:

1. On your domain controller, create a distribution point.
2. Log on to the server computer as an administrator.
3. Create a shared network folder where the FortiClient MSI installer file will be distributed from.
4. Set file permissions on the share to allow access to the distribution package. Copy the FortiClient MSI installer package into this share folder.
5. Select *Start* > *Administrative Tools* > *Active Directory Users and Computers*.
6. After selecting your domain, right-click to select a new Organizational Unit (OU).
7. Move all the computers you wish to distribute the FortiClient software to into the newly-created OU.
8. Select *Start* > *Administrative Tools* > *Group Policy Management*. The Group Policy Management MMC Snap-in will open. Select the OU you just created. Right-click it, *Select Create a GPO* in this domain, and Link it here. Give the new GPO a name then select *OK*.
9. Expand the Group Policy Object container and find the GPO you just created. Right-click the GPO and select *Edit*. The Group Policy Management Editor MMC Snap-in will open.
10. Expand *Computer Configuration* > *Policies* > *Software Settings*. Right-click *Software Settings* and select *New* > *Package*.
11. Select the path of your distribution point and FortiClient installer file and then select *Open*. Select *Assigned* and select *OK*. The package will then be generated.
12. If you wish to expedite the installation process, on both the server and client computers, force a GPO update.
13. The software will be installed on the client computer's next reboot. You can also wait for the client computer to poll the domain controller for GPO changes and install the software then.

Uninstall FortiClient using Microsoft Active Directory server:

1. On your domain controller, select *Start* > *Administrative Tools* > *Group Policy Management*. The Group Policy Management MMC Snap-in will open. Expand the Group Policy Objects container and right-click the Group Policy Object you created to install FortiClient and select *Edit*. The *Group Policy Management Editor* will open.
2. Select *Computer Configuration* > *Policy* > *Software Settings* > *Software Installation*. You will now be able to see the package that was used to install FortiClient.
3. Right-click the package, select *All Tasks* > *Remove*. Choose Immediately uninstall the software from users and computers, or *Allow* users to continue to use the software but prevent new installations. Select *OK*. The package will delete.
4. If you wish to expedite the uninstallation process, on both the server and client computers, force a GPO update as shown in the previous section. The software will be uninstalled on the client computer's next reboot. You can also wait for the client computer to poll the domain controller for GPO changes and uninstall the software then.

Deploy FortiClient using Microsoft SCCM 2012

The Microsoft System Center 2012 Configuration Manager (SCCM) may be used to deploy and manage multiple FortiClient Installations. This section presents various scenarios that you can utilize.

A fully functional SCCM server, along with discovered devices, is required. Visit the Microsoft web site for supporting documentation.

These instructions assume you have already installed and configured SCCM. If you have not, please refer to Microsoft's online help sources for information on this task.

The Microsoft *System Center 2012 Configuration Manager* (SCCM) may be used to deploy and manage multiple FortiClient Installations. This chapter presents various scenarios that you can utilize.

A fully functional SCCM server, along with discovered devices, is required. Visit the Microsoft web site for supporting documentation.

The following topics are detailed in this section:

- SCCM setup on page 28
- Task sequences on page 29
- Task sequence examples for FortiClient on page 40.

SCCM setup

Microsoft maintains a public free virtual lab of the *System Center 2012 Configuration Manager* (SCCM) at http://technet.microsoft.com/virtuallabs/bb539977.

At this page you can access a completely installed and properly configured system that can be used for testing various SCCM deployment scenarios. For ongoing enterprise use, a new system has to be created and configured.

The following subsections discuss some of the preparations required to enable control of FortiClient host computers.

Client discovery options and configuration

The uses various methods to discover the Windows devices that an administrator can control on the network. One such method is the use of a common domain. To use this method, the Windows server hosting the *Configuration Manager* should be configured as domain controller. All Windows devices that will be managed should then join the domain. The *Configuration Manager* automatically discovers all Windows devices that join.

Client installation

The *Configuration Manager* console may be used to install configuration manager client software on target Windows devices that have joined the controlled domain. This is required for pushing the configuration to the devices.

Client policy polling interval settings

The configuration manager client on each Windows device polls for policy changes on the server at a regular interval. The polling interval defaults to 60 minutes. Each newly pushed or deployed task will run on all selected clients within this polling interval. You can customize the polling interval as required.

Client collections

New configurations are usually deployed to collections of devices. All of the devices that have joined the controlled domain will be added to a default collection.

You may want to deploy a different set of configurations to different groups of devices based on your user base. This can be accomplished by creating different client collections. Devices that have joined the domain will be added to one or more of those collections. Configurations may then be selectively deployed.

Client security issues

The *Configuration Manager* is able to deploy a large variety of applications to all the devices that joined the domain. Most of these tasks run with the administrator or system user authorization level on the client devices. It is important to keep the *Configuration Manager* host under the highest level of security control possible.

It is also important to always test new planned application deployments in a controlled lab environment, or on a small client collection, before deploying to the entire client base.

Network share for all clients

The *Configuration Manager* console is used to deploy applications to client devices. Some of the applications require specification of files by file path and name. The client devices must have access to the files when the applications run. For instance, to upload a FortiClient XML configuration file to a given client collection, all client devices in the collection must independently have local access to the new XML configuration file.

The files may be provided by any suitable method. Examples include use of an HTTP or FTP server. The examples in this document use a network share. This should be available to all devices on the given client collection.

Task sequences

The *Configuration Manager* provides task sequences as a means of deploying commands to discovered clients without requiring user intervention. The FortiClient configuration examples in this chapter use the *Run Command Line* task sequences to run various command-line commands on client devices.

Here is a simple example of how task sequences may be used to control client devices.

In this example, a simple set of command-line commands are created in the *Configuration Manager* console. Once deployed, the commands will print information requested to the log file for each client.

The following commands will be executed on each client:

```
cd
dir c:\users
whoami
```

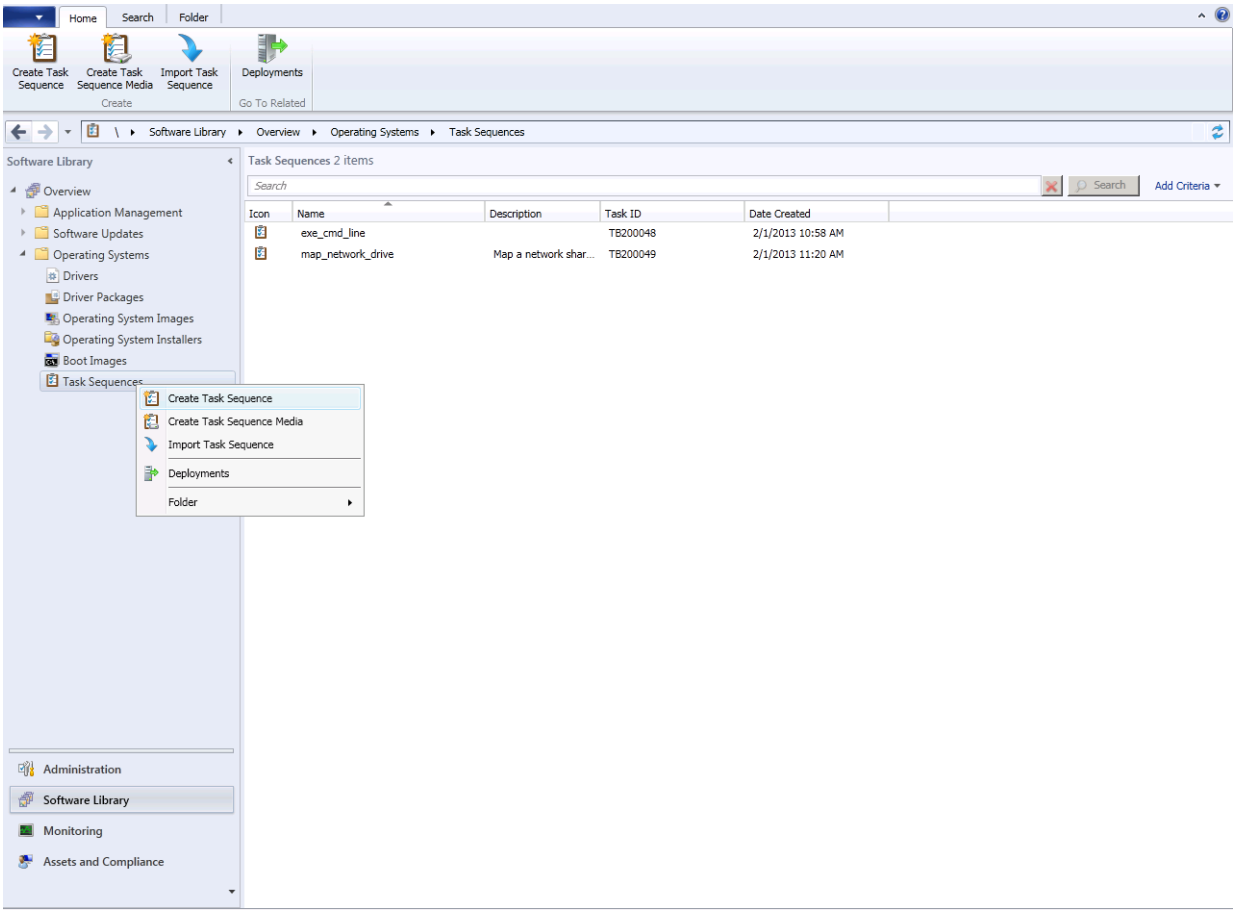
The first command will print the current working directory. This is likely to be `c:\windows\system32`. The second command will print the contents of the specified directory. The third command will print the name of the current user (the user under which the task sequence is running).

The output of the commands can be found in the log file on each client device at:

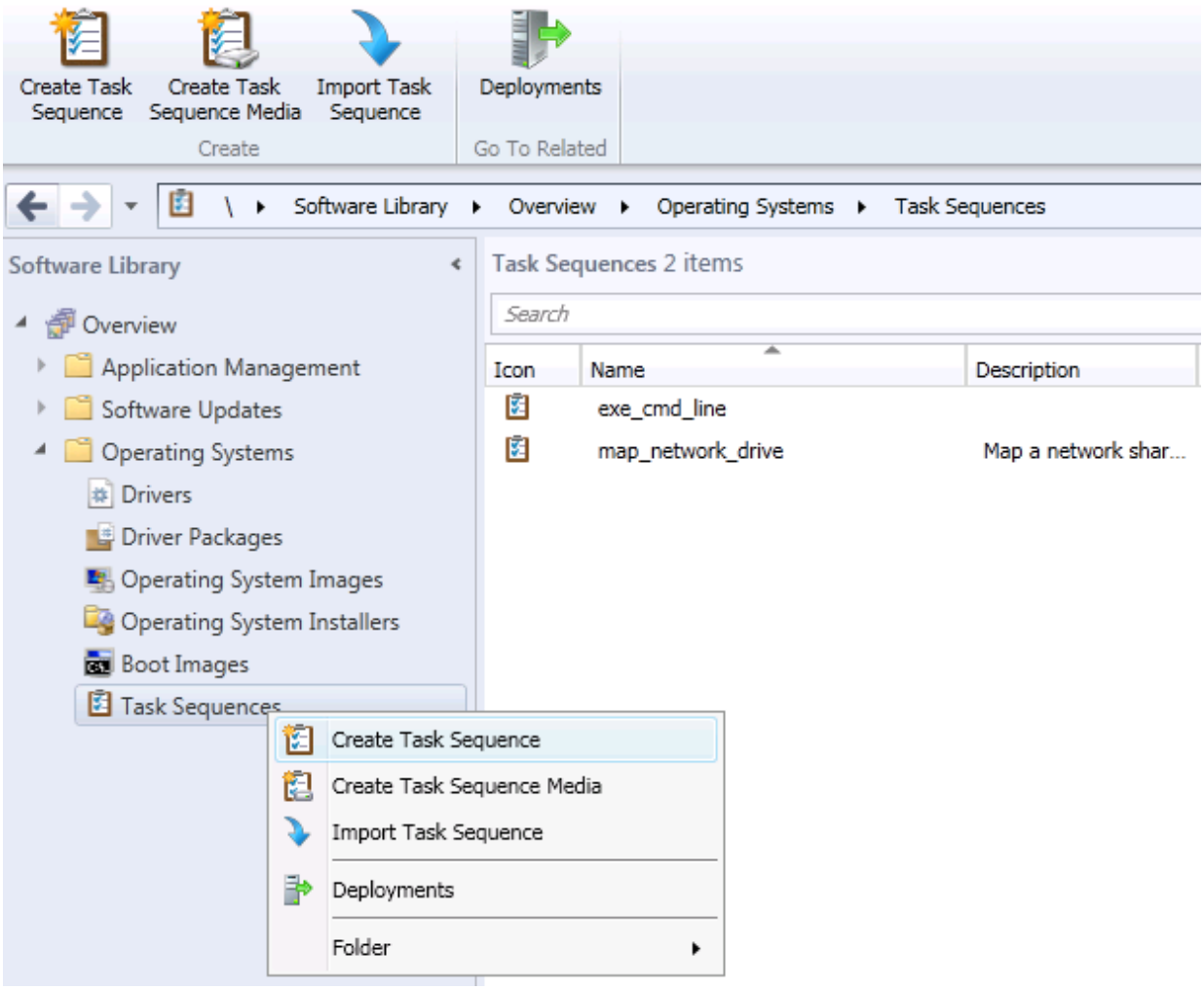
```
C:\Windows\CCM\Logs\smsts.log
```

To create a new task sequence:

1. Launch the *Configuration Manager* console. The *Configuration Manager* console opens.



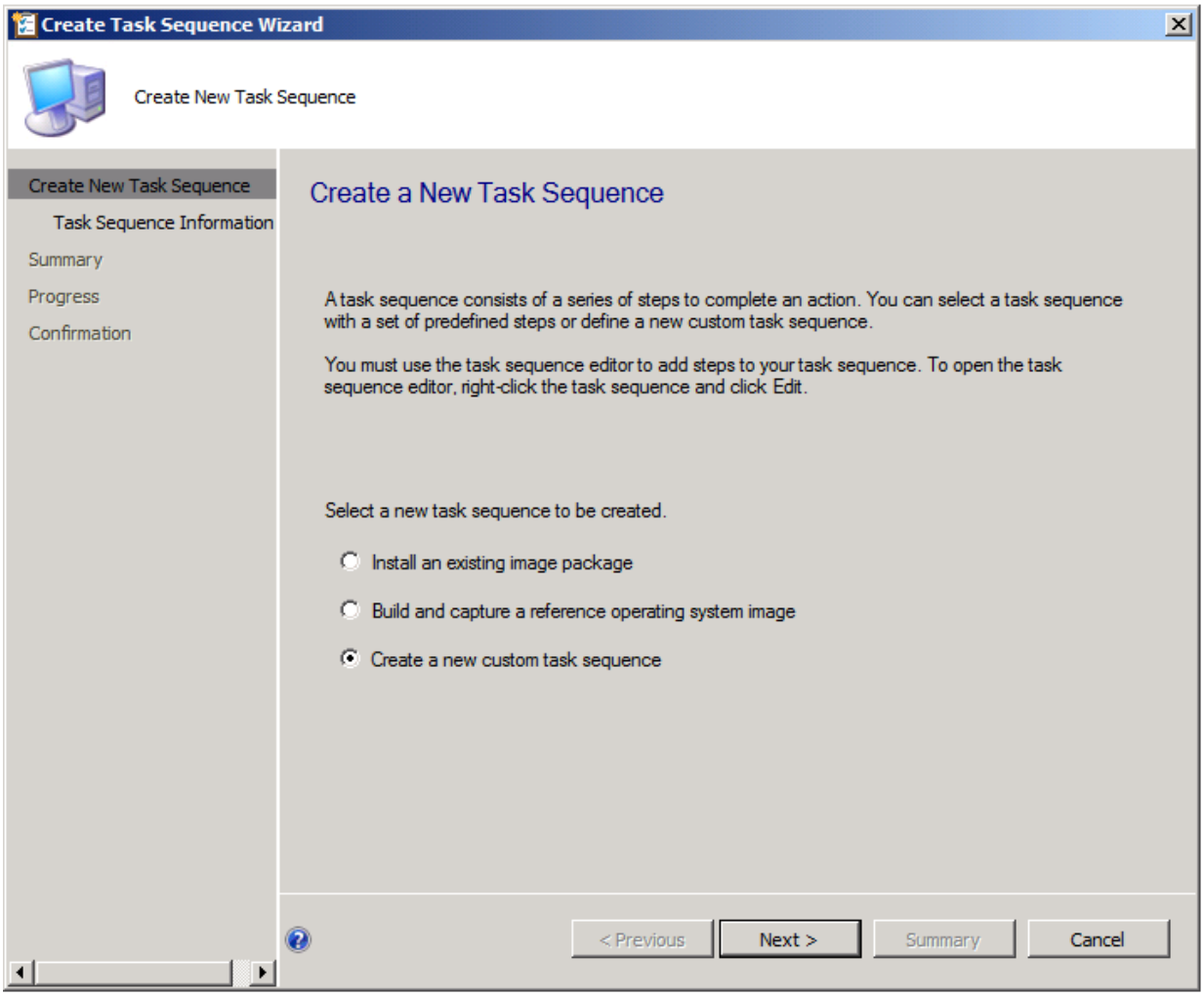
2. Select *Software Library* > *Overview* > *Operating Systems* > *Task Sequences*.
3. Right-click the *Task Sequence* menu item and select *Create Task Sequence*.



Alternatively, you can select *Create Task Sequence* in the toolbar.

The *Create Task Sequence Wizard* opens.

4. Create task sequence task wizard



5. Select the *Create a new custom task sequence* radio button. Then select *Next* to proceed.
6. Enter a name for the task sequence.
7. Enter a comment to describe the task sequence.
8. Select *Next* to proceed.

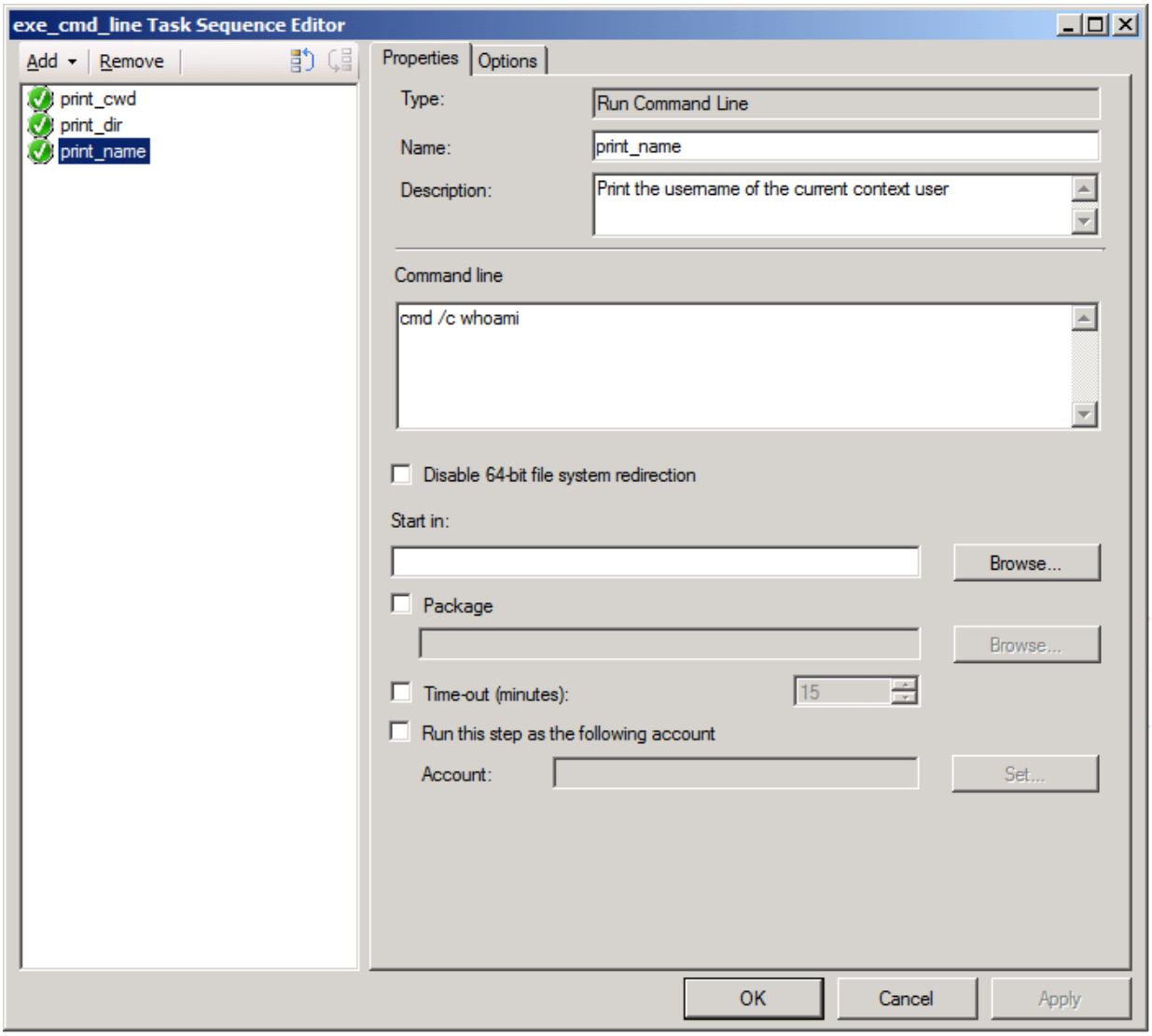
   A summary of the task sequence configuration is displayed.
9. Select *Close* to save the configuration. The new task sequence is created and displayed in the *Configuration Manager* console.
10. Select *Task Sequences* in the menu in the left pane of the *Configuration Manager* console. The new task sequence is displayed in the right pane.

To add individual tasks into the task sequence:

1. Right-click in the newly created task sequence.
2. From the shortcut menu list, select *Edit*. The *Task Sequence Editor* dialog box is displayed.

   Alternatively, select the *Task Sequence* and select the *Edit* icon in the toolbar.
3. Select the *Add* drop-down button.
4. From the drop-down list, select *General* and the select *Run Command Line.*

A new tab is displayed in the right pane of the dialog box.



5. Configure the following settings:

Name	Enter a name for the command.
Description	Enter a description for the command.

Command line	Enter the command line in the text field.
	The command will usually start with “cmd /c”. For instance, the first command in this example is entered as:
	`cmd /c cd`
	`cmd /c dir c:\users`
	`cmd /c whoami`

6. Select *Apply* to apply the configuration.
7. Select OK to continue.

The task sequence will be saved with the three command-line tasks. To view or modify the tasks, select *Edit* in the short-cut menu for the selected task sequence.

There are three commands in this example. Each of the commands may be created as a single task. There will be a total of three tasks in the left pane of the dialog box. Each of the tasks will have one of the command-line commands:

```
cmd /c cd
cmd /c dir c:\users
cmd /c whoami
```

This format is preferred as it isolates any client errors to a specific task.

The three commands may also be combined into a lengthy single command:

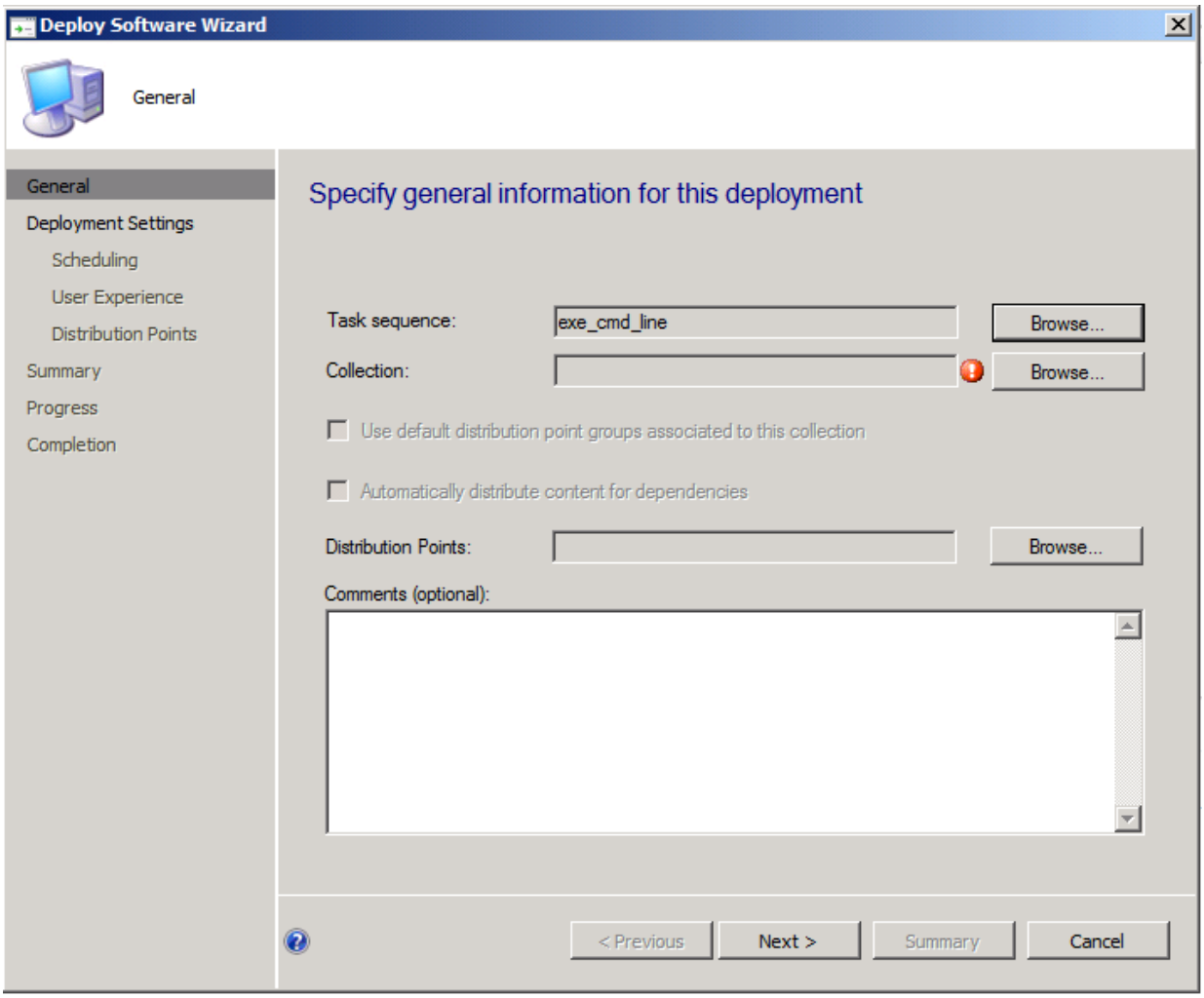
```
cmd /c cd ; dir c:\users ; whoami
```

This format may mask task sequence errors. It is not recommended.

There is also an option to use a batch script.

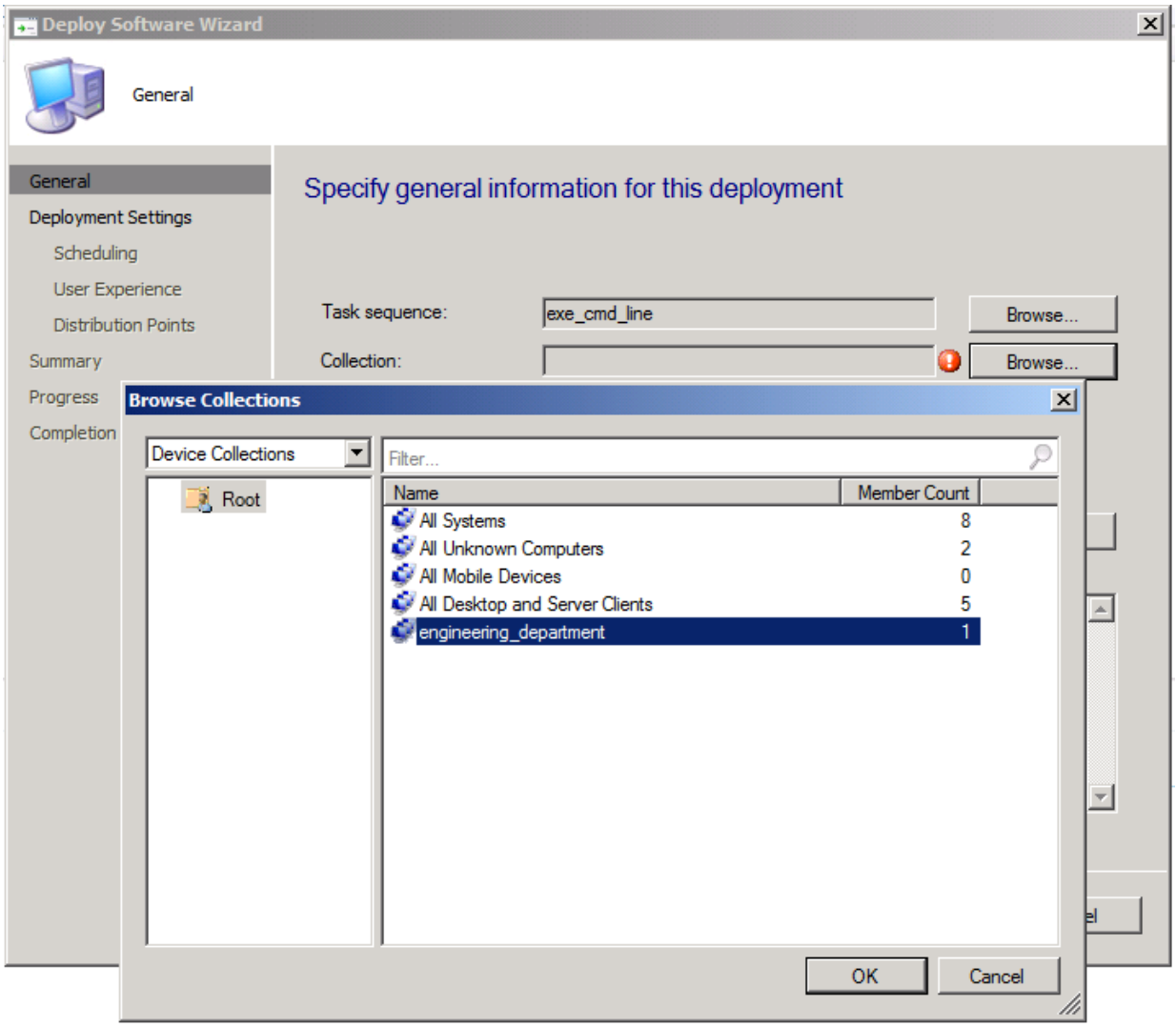
Deploy the task sequence:

1. Right-click the task sequence.
2. Select *Deploy* in the right-click menu list. The *Deploy Software Wizard* dialog box opens.



Alternatively, select the *Task Sequence* and select the *Deploy* icon in the toolbar.

3. Select *Browse*.
   A *Browse Collections* dialog box appears listing all currently configured client collections.



4. Select the client collection to which this task sequence should be deployed
5. Select *OK* to close the *Browse Collections* dialog box. Pressing CTRL returns you to the *General* tab of the *Deploy Software Wizard* dialog box.
6. Select *Next*. The *Deployment Settings* tab is displayed
7. In the *Purpose* drop-down menu select *Required*. This makes the task mandatory for all clients receiving it.
8. Select the *Send wake-up packets* checkbox to enable this feature.
9. Select *Next*. The *Scheduling* tab is displayed
10. Select *New*. In the *Assignment Schedule* dialog box select the *Assign immediately after this event* radio button.
11. Select *OK*. This closes the *Assignment Schedule* dialog box. The *Scheduling* tab is displayed.
12. Select *Next*. The *User Experience* tab is displayed.
13. Select the *Show Task Sequence progress* checkbox to enable this feature.

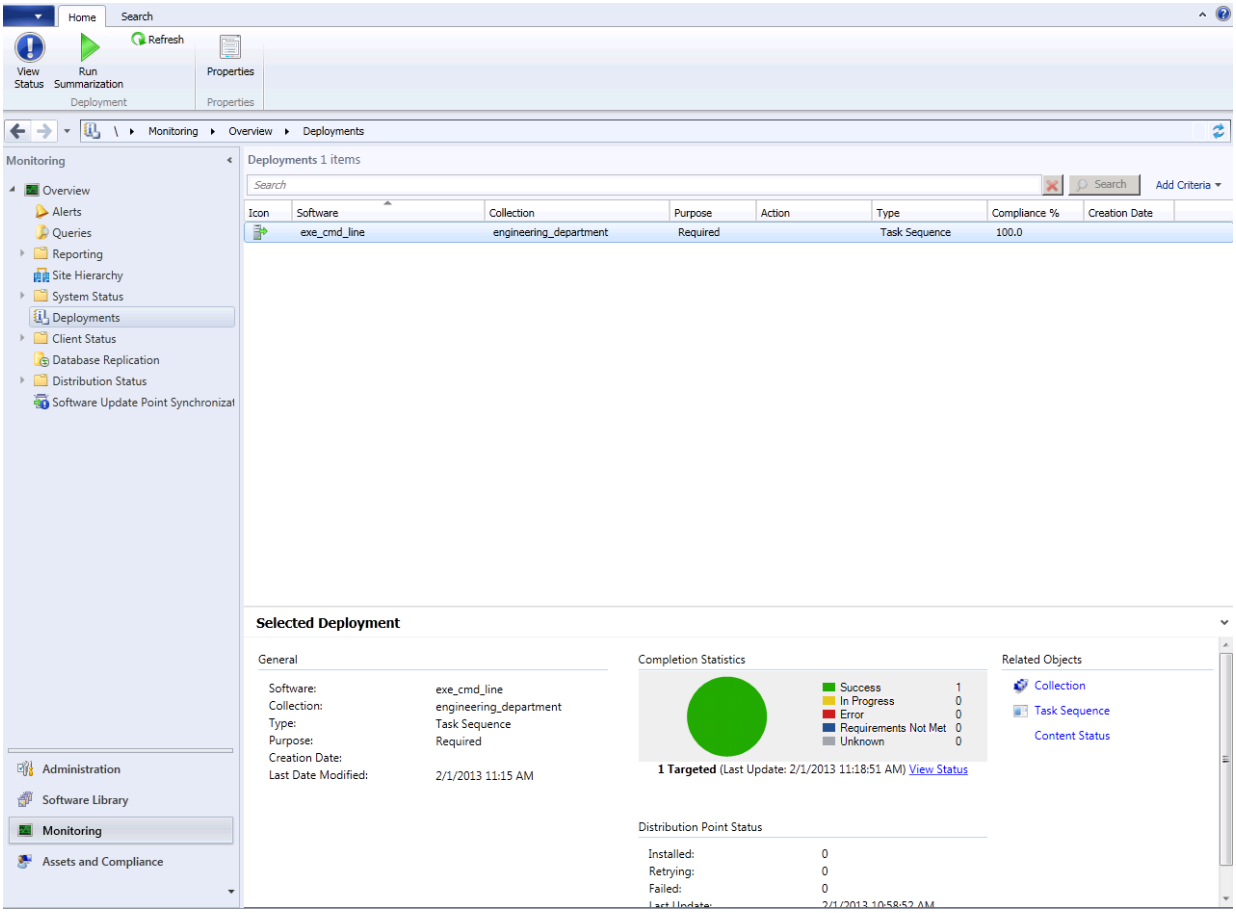
    This configuration is optional. It displays a progress dialog box on each client as the task executes. If a silent background execution of tasks is desired, leave this checkbox unchecked.
14. Select *Next*. The *Distribution Points* tab is displayed. For this example, there is nothing to change in this tab.
15. Select *Next*. The *Summary* tab is displayed.

16. Select *Next*. The *Completion* tab is displayed which shows a summary of all selections.
17. Select *Close* to close the *Deploy Software Wizard*.

    This completes the deployment of the task sequence to the selected client collections. Client devices in the collection should start to receive and execute the task. All clients will run the task within the *Policy Polling Interval* configured.

Monitor a deployed task sequence:

1. Launch the *Configuration Manager* console.
2. Select *Monitoring* from the tree-menu.
3. Select the *Overview* menu item in the left pane to expand the menu.
4. Select the *Deployments* menu item. The list of deployments is displayed in the right pane.
5. Click to select the recently deployed task sequence in the right pane. The *Deployments* window is displayed.



To monitor a deployed task sequence on the client device, use the following process:

1. Launch the *Software Center* console on the client device. It displays a list of tasks deployed to it.

If a recently deployed task sequence is not displayed, most likely the *Policy Polling Interval* is yet to expire on this client.

2. Select the *Task Sequence*. The current status is displayed.

In addition to the two monitoring procedures above, the client log file is available on the client device at:

```
C:\Windows\CCM\Logs\smsts.log
```

It will contain details of the task sequence, including:

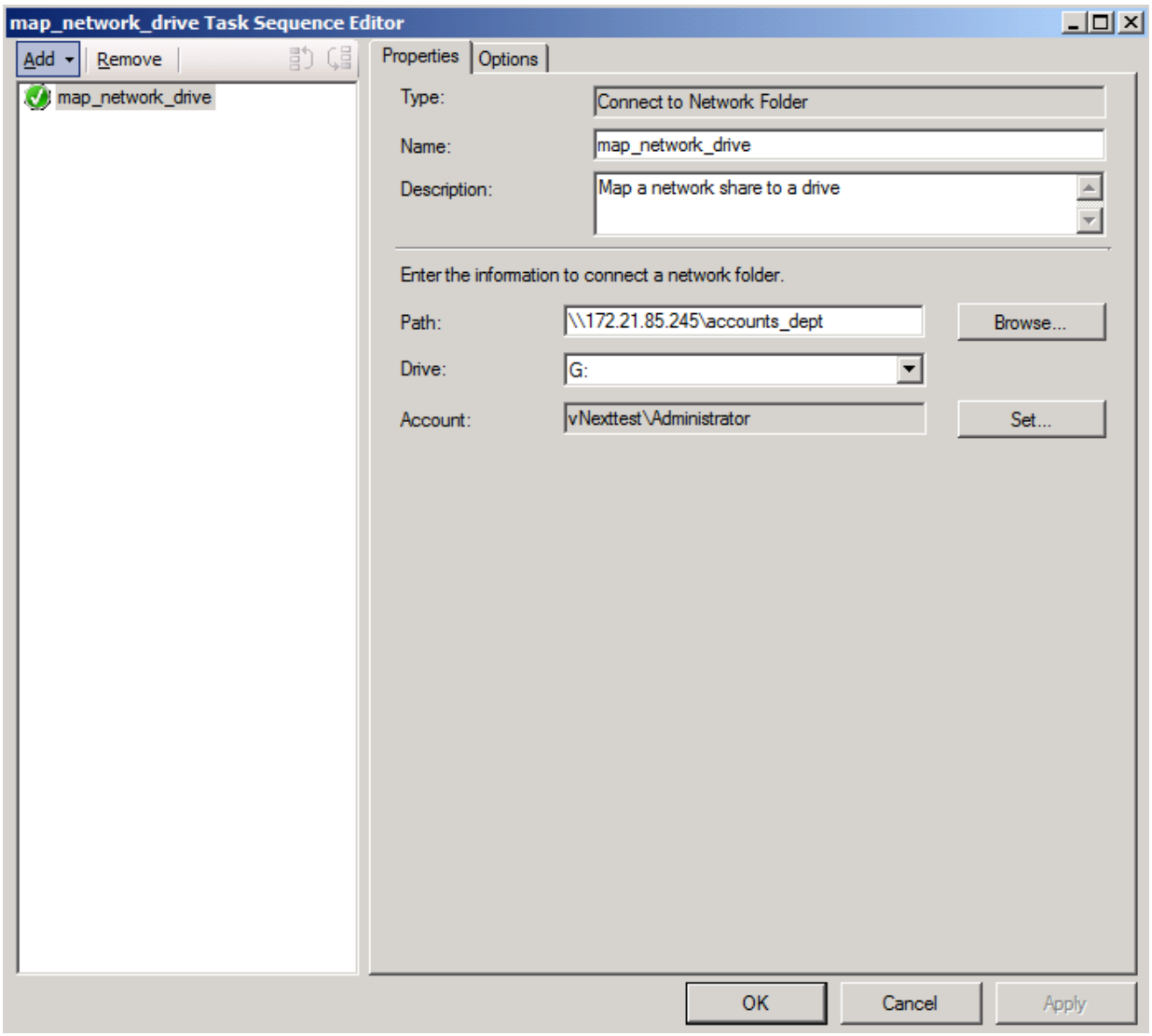
- the command-line commands executed
- any output generated by the commands
- any error messages.

Map a network drive

When a file is referenced in a task sequence, it must be made available to all clients before the task sequence starts. The processes listed below explain how to map a network folder to a drive in a given task sequence. If the mapping is successful, all the files in the shared folder will be available for the command-line commands in the task sequence.

To map a network drive in the task sequence:

1. Create a new custom task sequence.
2. Edit the task sequence. The *Task Sequence Editor* dialog box is displayed.



3. Select the *Add* drop-down button.
4. In the drop-down list, select *General* > *Connect to Network Folder*. A new tab is displayed in the right pane of the dialog box.
5. Type a name for the command.
6. Type a description for the command.
7. Type the full path to the network shared folder or use the *Browse* button to select it.

When using the *Browse* button, be sure that the network share is being reported with the same path as the client devices will use.

Here is an example of a valid path: \\172.21.85.245\accounts_dept

8. Type a drive letter, along with a colon.
   For example: G:
9. Select *Set* and provide a user name and password that is valid for the network shared folder selected.

10. Select *OK* to return to the *Task Sequence Editor* dialog box.
11. Select *Apply* to save the task.

    More tasks may be added to the task sequence as described in earlier parts of this section. Tasks may be re-ordered using the other buttons provided in the top of the left pane in the *Task Sequence Editor* dialog box.

    When all tasks have been added, select *OK* to close the dialog box.

Task sequence examples for FortiClient

The task sequence processes described in the preceding section may be applied to any regular Windows tasks that runs on the command line. This section discusses several example FortiClient configurations that could be completed from the Windows command-line.

The examples in this section list only the command-line commands to be used. When deploying these from the *Configuration Manager* console, remember to always use the processes discussed this chapter to create the task sequence. The procedure is the same, only the contents of the *Run Command Line* commands will differ.

Install FortiClient

FortiClient can be installed from the command line using `msiexec`. In this example, a FortiClient MSI file that is provided on a network shared folder is used to install FortiClient to devices in the client collection.

Use the following commands in a task sequence to install FortiClient on a Windows client device.

1. Connect to a network folder:
   - Name: `map_network_drive`
   - Description: Mount a network shared directory that contains the FortiClient image to install
   - Path: \\172.21.85.245\accounts_dept
   - Drive: G:
   - Account: `vNexttest\administrator`
2. Run command line:
   - Name: `copy_fct_image`
   - Description: Copy FortiClient MSI image from network shared directory
   - Command line: `cmd /c copy /y G:\FortiClient.msi c:\temp\FortiClient.msi`
3. Run command line:
   - Name: `install_fct`
   - Description: Install FortiClient using MSI image
   - Command line: `cmd /c msiexec /i c:\temp\FortiClient.msi /qn`

Ensure that the FortiClient.msi file is available in the network share, and that the network share is accessible to all client devices in the client collection before deploying this task sequence.

Export the FortiClient XML configuration file

FortiClient features may be controlled using an XML configuration file. The configuration file is first exported from FortiClient, modified with a text editor, and re-imported into FortiClient. The XML configuration syntax and usage is documented in the *FortiClient v5.2 XML Reference*.

Use the following commands in a task sequence to export the XML configuration file from a Windows client device which has FortiClient installed.

1. Connect to a network folder:
   - Name: map_network_share
   - Description: Mount a network shared directory to which configuration file will be copied.
   - Path: \\172.21.85.245\engineering_dept
   - Drive: M:
   - Account: vNexttest\administrator
2. Run command line:
   - Name: export_fct_xml
   - Description: Export the FortiClient XML configuration file
   - Command line: cmd /c C:\Program Files\Fortinet\FortiClient\fcconfig -o export -f c:\temp\fct_xml.conf
3. Run command line:
   - Name: copy_fct_xml
   - Description: Copy FortiClient XML file to network shared directory
   - Command line: cmd /c copy /y c:\temp\fct_xml.conf M:\

This copies fct_xml.conf to the mounted share. If there is more than one device in the client collection, they will each overwrite the same file. You may use a batch script to uniquely rename the file as it is copied.

The full path to the FortiClient installation directory is used as a prefix to FCConfig.exe. The value provided in this example is the default on a 32-bit system. The default on 64-bit systems is:

```
C:\Program Files (x86)\Fortinet\FortiClient
```

If the client collection has a mixture of both 32-bit and 64-bit devices, a batch script may be used to selectively run from the correct platform-dependent directory.

Import a modified XML configuration file

Use the following commands in a task sequence to import an XML configuration file into FortiClient in a Windows client device.

1. Connect to a network folder:
   - Name: map_network_share
   - Description: Mount a network shared directory that contains the XML configuration file
   - Path: \\172.21.85.245\engineering_dept
   - Drive: M:
   - Account: vNexttest\administrator
2. Run command line:
   - Name: copy_fct_xml
   - Description: Copy FortiClient XML configuration file from network shared directory
   - Command line: cmd / c copy /y M:\fct_xml.conf c:\temp\
3. Run command line:
   - Name: import_fct_xml
   - Description: Import the FortiClient XML configuration file
   - Command line: cmd /c “C:\Program Files\Fortinet\FortiClient\fcconfig -o import -f c:\temp\fct_xml.conf”

   The same configuration file is used by all devices in the client collection.

When deploying a custom FortiClient XML configuration, use the advanced Endpoint Profile options in FortiGate to ensure the Endpoint Profile settings do not overwrite your custom XML settings. For more information, see the *FortiClient v5.2 XML Reference* and the *CLI Reference for FortiOS 5.2*.

Upgrade FortiClient

The FortiClient upgrade process is similar to the regular installation. The only difference is the use of a different version of FortiClient during the installation. A reboot is required, but the task sequence should handle this properly.

The same procedure listed earlier for FortiClient installation could be reused.

Uninstall FortiClient

Use the following command in a task sequence to uninstall FortiClient from Windows client devices.

1. Run command line:
   - Name: uninstall_fct
   - Description: Uninstall FortiClient
   - Command line: wmic product where name="FortiClient" call uninstall /nointeractive

   The task sequence should process the required reboot correctly.

Endpoint Management

Introduction

The purpose of this section is to provide basic instructions on how to configure, deploy, and manage FortiClient configurations from your FortiGate device.

Endpoint Management is available on FortiGate 30D model series and higher.

Endpoint Management requires FortiClient v5.0/v5.2 and a FortiGate device running FortiOS v5.0/v5.2, or a FortiCarrier device running FortiOS Carrier v5.0/v5.2.

FortiOS v5.2 can manage both FortiClient v5.2 and FortiClient v5.0 registrations. Certain features are only available in FortiClient v5.2.

Configure endpoint management

In FortiOS 5.0 or later, configuration and management of FortiClient endpoint agents are handled by FortiGate. You can configure your FortiGate device to discover new devices on your network, enforce FortiClient registration, and deploy a pre-configuredFortiClient profile to connected devices. The FortiClient profile can be deployed to devices on your network and over a VPN connection. You can configure multiple FortiClient profiles. The FortiClient profile consists of the following sections:

- Antivirus Protection
- Web Category Filtering

  You can select the web filtering security profile to associate with the FortiClient profile. You can also select to enable Web Filtering when the client is protected by the FortiGate (On-Net).
- VPN

  Select to enable client VPN provisioning. You can specify the VPN name, type, gateway and other settings the client will use to connect to your FortiGate device via the VPN connection. Two-factor authentication is configured in the FortiGate VPN configuration.
- Application Firewall

  You can select the application control sensor to associate with the FortiClient profile.
- Endpoint Vulnerability on Client

  You can select to scan daily, weekly or monthly. You can also select to scan the client after registration with your FortiGate device. Vulnerability Scan must be enabled via the CLI in order for it to be displayed in the FortiClient Profile.
- Upload logs to FortiAnalyzer/FortiManager

You can select to use the same IP address as the FortiGate device or specify a different device IP address. You can specify the frequency of the log upload. FortiClient must be registered to FortiGate to upload logs to FortiAnalyzer/FortiManager.

- Use FortiManager for client software/signature update

  Select to enable this feature and enter the IP address of your FortiManager device. You can select to failover over to the FortiGuard Distribution Network (FDN) when the FortiManager is not available.

- Dashboard Banner

  You can select to display or hide the FortiClient advertisement banner. FortiClient ads are downloaded from the FortiGuard Distribution Servers.

  Select if profile details may be displayed before endpoint control registration is completed.

- Client-based Logging when On-Net

  Select to enable client-based logging when protected by the FortiGate (On-Net).

When FortiClient is On-Net, the icon displayed to the left of the username will be green. When FortiClient is Off-Net, the icon is grey.

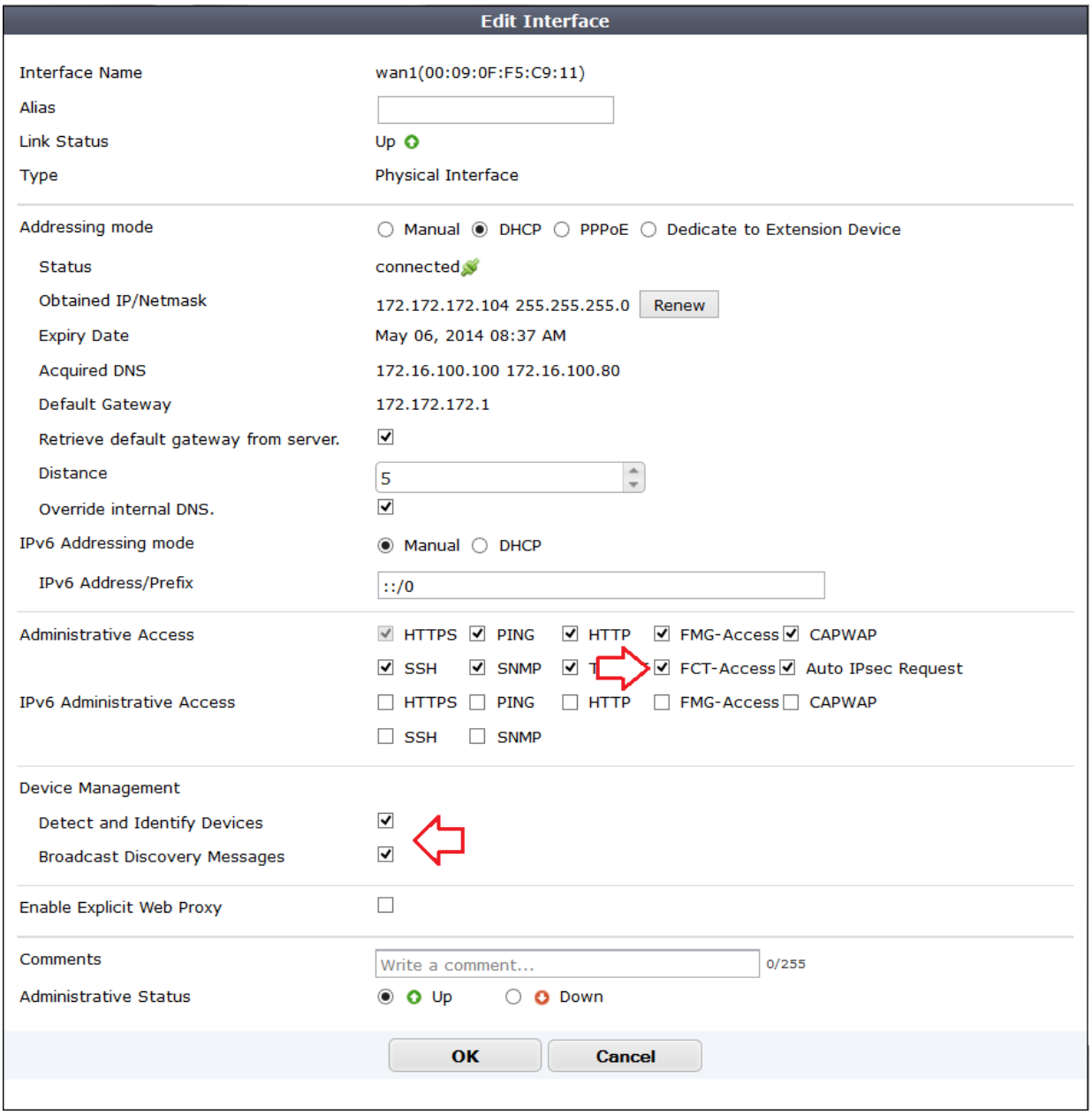
See the *FortiOS Handbook* for more information on configuring your FortiGate device.

Configure Endpoint Management on the FortiGate device:

1. Enable device management and broadcast discovery messages.

   To configure *Device Management*, go to *System* > *Network* > *Interfaces*, select the applicable interface, then select *Edit* in the toolbar. In the *Edit Interface* page you can select to enable *Detect and Identify Devices*. To enable *Broadcast Discovery Messages* (optional) you must first enable *FCT-Access* under *Administrative Access*. Select *OK* to save the setting.

Broadcast Discovery Messages is an optional configuration. When enabled, the FortiGate will broadcast messages to your network, allowing client connections to discover the FortiGate for FortiClient registration. Without this feature enabled, the user will enter the IP address or URL of the FortiGate to complete registration.

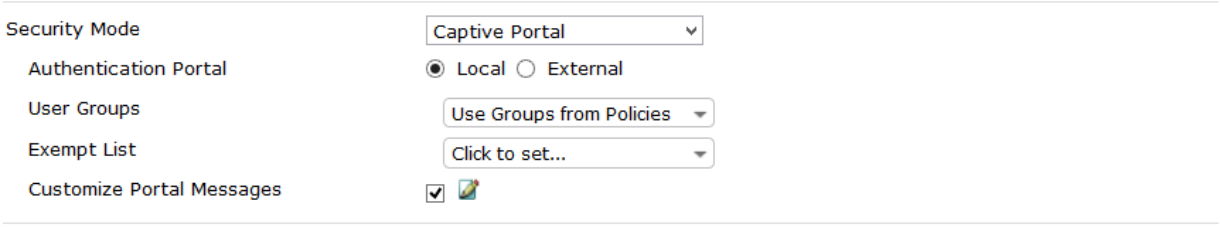


2. Configure the following settings:

Administrative Access	Select the checkbox for FCT-Access. This option is available for both IPv4 and IPv6 Administrative Access.
Security Mode	Select None or Captive Portal. When selecting Captive Portal, users are forwarded to a captive portal where they need to enter their username and password to authenticate with the FortiGate. You can customize the portal message and specify user groups. This option is available when Addressing mode is set to Manual.
Device Management	

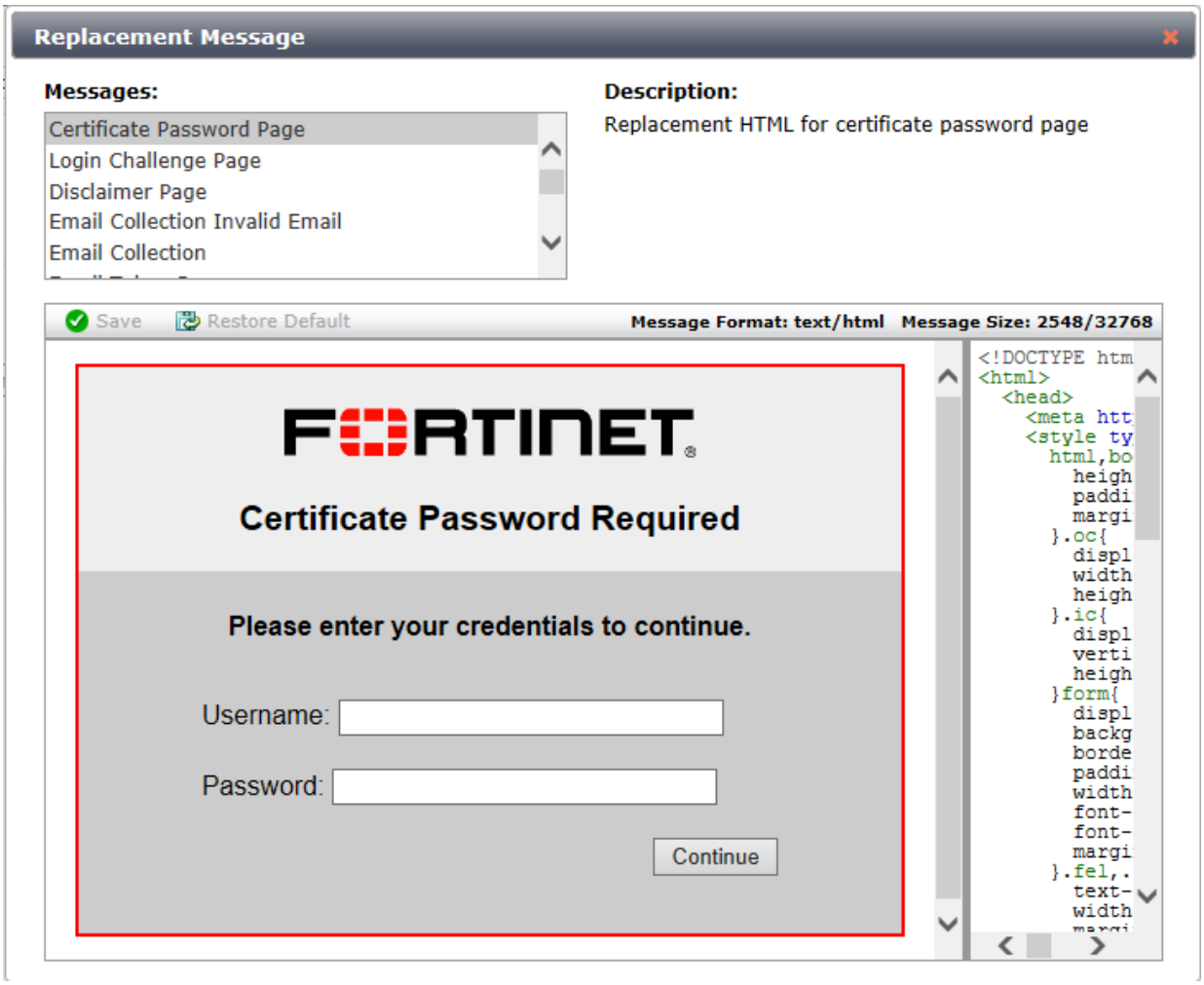
Detect and Identify Devices	Select to detect and identify devices on the selected interface.
Broadcast Discovery Messages	Once enabled, the FortiGate unit broadcasts a discovery message that includes the IP address of the interface and listening port number to the local network. All PCs running FortiClient on that network listen for this discovery message. This option is available when *FCT-Access* is enabled.

When configuring FortiClient access on an internal interface, you can select to send users to a captive portal.



Security Mode	Select *Captive Portal* from the drop-down list
Authentication Portal	Select either *Local* or *External*. When selecting *External*, you can specify the link path.
User Groups	Select user groups from the drop-down list. FortiClient does not support nested groups in FortiOS.
Exempt List	Select an exempt list from the drop-down list.
Customize Portal Messages	Enable and select the edit icon to edit the portal replacement message.

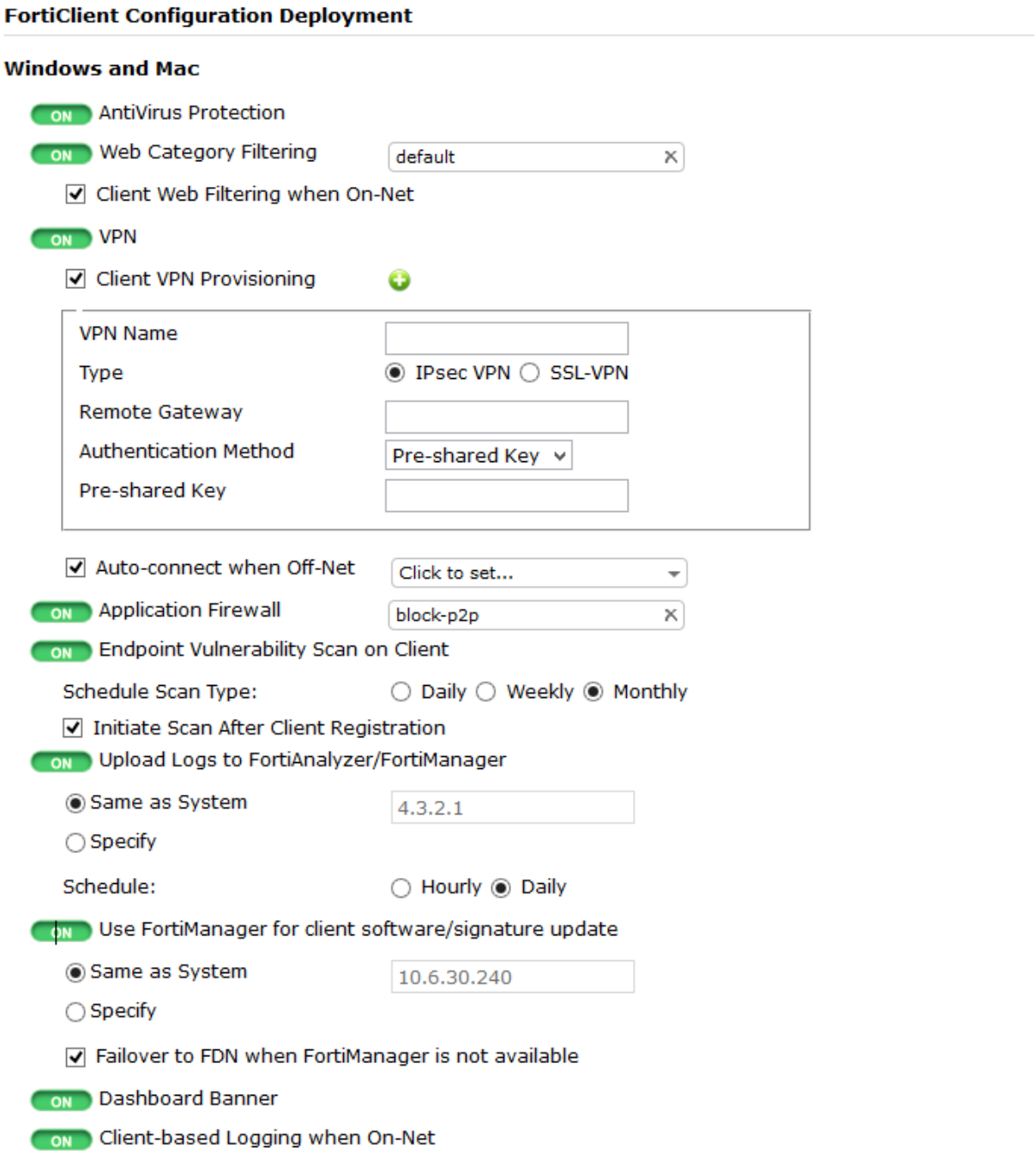
The following dialog box shows the captive portal replacement message editor.



Configure the FortiClient profile:

1. To configure the *FortiClient Profile*, go to *User & Device* > *FortiClient Profiles*. You can edit the default profile or create a new FortiClient profile.

	The option to assign the profile to device groups, user groups, and users is only available when selecting to create a new FortiClient profile. You can assign the profile to user groups and users when using Active Directory authentication or RADIUS authentication for VPN.
	In FortiOS v5.0.3 or later, you will need to enable *Multiple Security Profiles* in the *Feature Settings* to create a new FortiClient profile.
	When registering to a FortiGate device, FortiClient will receive the configured FortiClient profile. The FortiClient configuration is overwritten by the FortiClient profile settings. When selecting to unregister FortiClient, the settings will reflect that of the FortiClient profile.



2. Configure the following settings:

Toolbar Options	**FortiClient Profile page** Select *Create New* to create a new FortiClient profile. Select a profile in the list and select *Edit* to edit the FortiClient Profile. Select a profile in the list and select *Delete* to delete the FortiClient Profile. **Edit FortiClient Profile page** Select the create new icon to create a new FortiClient profile. Select the clone icon to create a clone of an existing FortiClient profile. Select the view list icon to view FortiClient profiles and assignment.
Profile Name	When editing the default profile, the name cannot be changed. When creating a new FortiClient profile, XSS vulnerability characters are not allowed. Enter a name for the new FortiClient profile.
Comments	Enter a profile description. (optional)
Assign to Profile To:	Device Groups: Select device groups in the drop-down list. Use the add icon to assign multiple device groups to the FortiClient profile, for example Mac and Windows PC. • User Groups: Select user groups in the drop-down list. Use the add icon to assign multiple user groups to the FortiClient profile. • Users: Select users in the drop-down list. Use the add icon to assign multiple users to the FortiClient profile. These options are only available when creating a new FortiClient profile. You can assign the profile to user groups and users when using Active Directory authentication or RADIUS authentication for VPN. FortiClient does not support nested groups in FortiOS.
FortiClient Configuration Deployment - Windows and Mac	
AntiVirus Protection	Toggle the button on or off to enable or disable this feature.
Web Category Filtering	Toggle the button on or off to enable or disable this feature. When enabled, you can select a web filter profile in the drop-down list. Select the checkbox to disable web category filtering on the client when protected by the FortiGate (On-Net).
VPN	Toggle the button on or off to enable or disable this feature. Select the checkbox for Client VPN Provisioning. When enabled, you can configure multiple IPsec VPN and SSL VPN connections. Use the add icon to add additional VPN connections. Enter the VPN name, type, remote gateway, and authentication method information. Select the checkbox to auto connect to a VPN when the client is Off-Net. Select a VPN from the drop-down list.
Application Firewall	Toggle the button on or off to enable or disable this feature. When enabled, you can select an application control sensor in the drop-down list.

Endpoint Vulnerability Scan on Client	Toggle the button on or off to enable or disable this feature. When enabled, you can select the scheduled scan type to daily, weekly, or monthly. Select the checkbox to initiate a scan after client registration with the FortiGate. Vulnerability Scan must be enabled via the CLI in order for it to be displayed in the FortiClient Profile.
Upload Logs to FortiAnalyzer/FortiManager	Toggle the button on or off to enable or disable this feature. When enabled, you can select to use the same FortiAnalyzer/FortiManager used by the FortiGate or select *Specify* to enter a different device IP address. You can set the schedule to hourly or daily. The FortiClient upload logs to the FortiAnalyzer/FortiManager only when it is able to connect to the device on the specified IP address. FortiClient must be registered to FortiGate to upload logs to FortiAnalyzer/FortiManager. When upgrading from FortiOS v5.0 to v5.2, a FortiClient v5.2 license must be applied against the FortiGate for this option to be available in the FortiClient Profile. Optionally, you can enable this setting in the FortiOS CLI.
Use FortiManager for client software/signature update	Toggle the button on or off to enable or disable this feature. When enabled, you can specify the IP address of the FortiManager. Select the checkbox to failover to the FortiGuard Distribution Network when the FortiManager is not available.
Dashboard Banner	Toggle the button on or off to enable or disable this feature.
Client-based Logging when On-Net	Toggle the button on or off to enable or disable this feature.

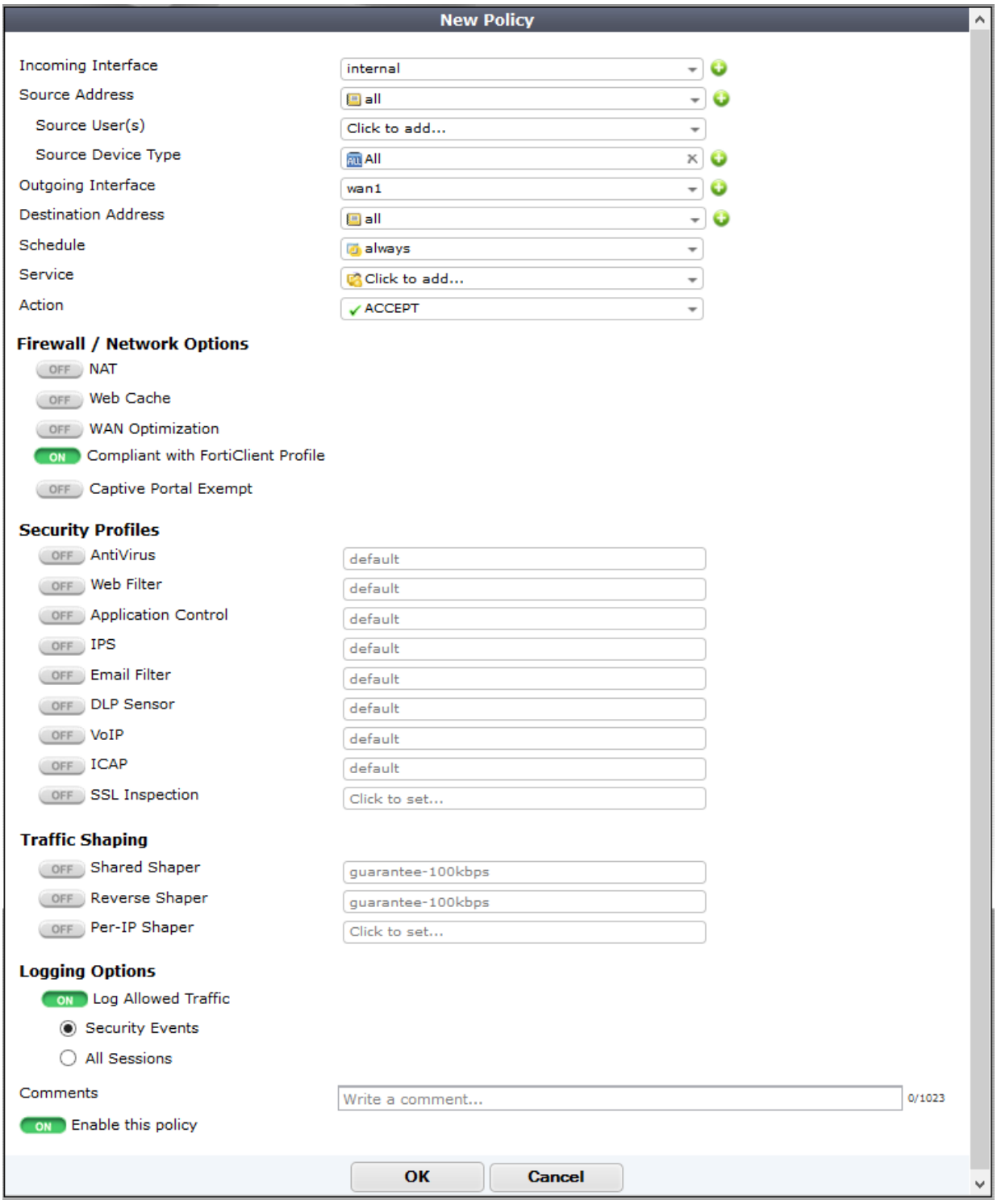
3. Select *Apply* to save the FortiClient profile setting.

When deploying a custom FortiClient XML configuration, use the advanced FortiClient Profile options in FortiGate to ensure the FortiClient Profile settings do not overwrite your custom XML settings. For more information, see the *FortiClient XML Reference* and the *CLI Reference for FortiOS*.

For information on configuring firewall policies for Endpoint Management, see the *FortiOS Handbook - The Complete Guide for FortiOS*.

Configure firewall policies (Optional):

1. To configure a firewall policy for *Endpoint Management*, go to *Policy & Objects* > *Policy* and select *Create New* in the toolbar. The *New Policy* window is displayed.



2. Configure the policy as required. Select the source user(s) and source device types from the drop-down list.
3. Toggle *Compliant with FortiClient Profile* to *ON*. Users will be redirected (via a web browser) to a dedicated portal where they can download the client. Once registered to the FortiGate, the FortiClient profile will be assigned.

You can create policies for users and devices which will be captive portal exempt.

When creating a device policy, if *Device Management* > *Detect and Identify Devices* is not enabled on the incoming interface you will be prompted a confirmation dialog box with the option to *Enable Device Identification*.

4. Select *OK* to save the rule.

   After the FortiGate configuration has been completed, you can proceed with FortiClient configuration. Configure your Windows PC on the corporate network with the default gateway set to the IP address of the FortiGate.

FortiClient endpoint network topologies

The following FortiClient Profile topologies are supported:

1. Client is directly connected to FortiGate; either to a physical port, switch port or WiFi SSID.

   This topology supports client registration, configuration sync, and FortiClient profile enforcement.

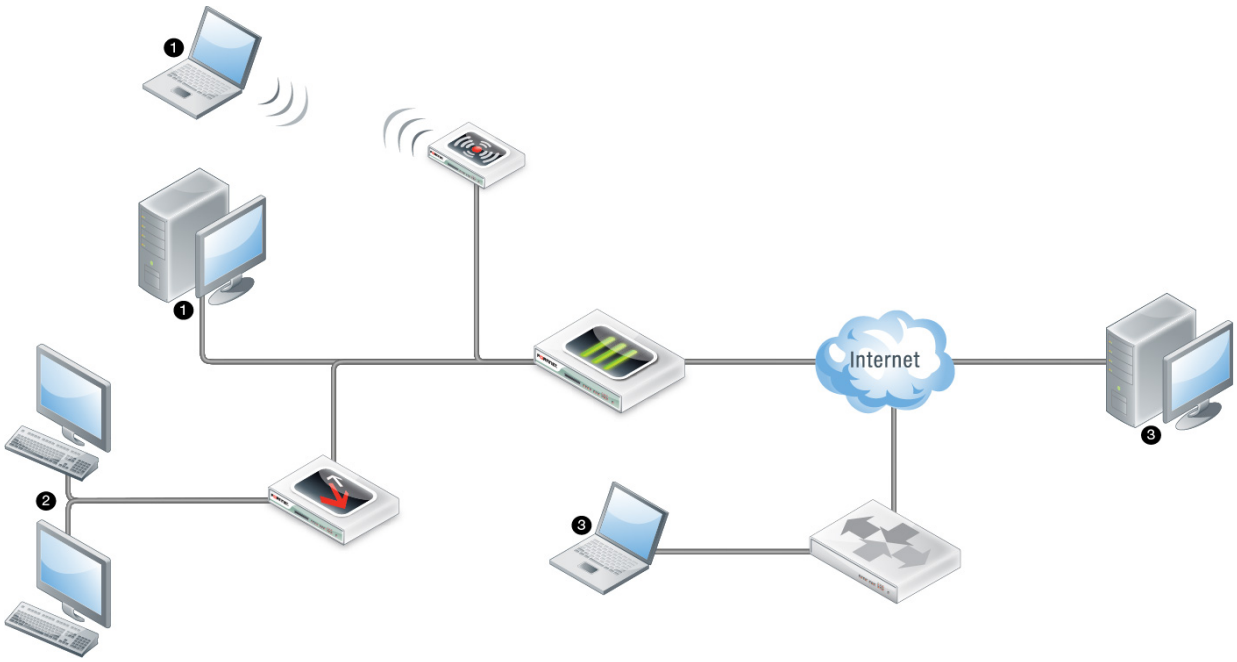
2. Client is connected to FortiGate, but is behind a router or NAT device.

   This topology supports client registration and configuration sync.

3. Client is connected to FortiGate across a VPN connection.

   This topology supports client registration, configuration sync, and FortiClient profile enforcement.

Network topologies

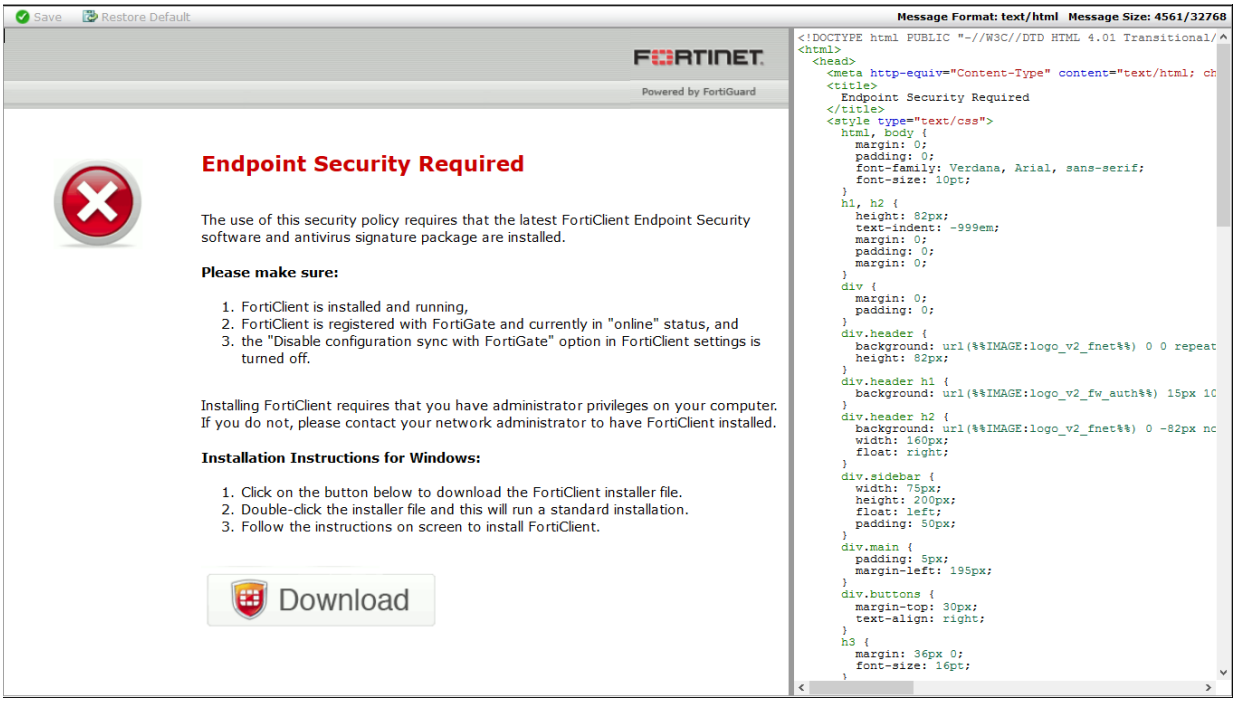


Configure FortiClient for Endpoint Management:

1. Download and install the FortiClient software.

   Open a web browser from your workstation and attempt to open a web page, the web page will be directed to the *NAC Download Portal*. Follow the instructions in the portal to download and install FortiClient.

To allow users to download FortiClient, you must enable this setting in the *SSL VPN Portal* on your FortiGate device. To enable this feature, go to *VPN* > *SSL* > *Portals* and select *Create New* in the toolbar.



To configure NAC download portal endpoint control replacement messages, go to *System* > *Config* > *Replacement Message*. Select *Extended View* in the toolbar to display *Endpoint Control* replacement messages for Android, iOS, Mac, Windows, and other.

2. Register FortiClient.

   After FortiClient completes installation, FortiClient will automatically launch and search for a FortiGate device for registration.

   There are four ways that the FortiClient/FortiGate communication is initiated:

   - FortiClient will attempt to connect to the default gateway IP address;
   - FortiClient will attempt endpoint control registration over VPN (if configured on the FortiGate);
   - FortiClient will attempt to connect to a remembered FortiGate;
   - FortiClient will attempt to connect to a redundant FortiGate.

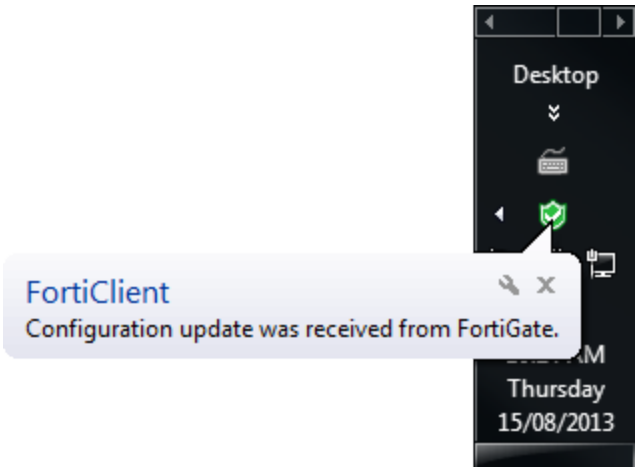
   Your personal computer's default gateway IP address should be configured to be the IP address set in the FortiGate interface.

   FortiClient will search for available FortiGate devices to complete registration. You can include the option to prompt the user to enter the FortiClient registration key password. Select the *Register to FortiGate* button in the FortiClient console to retry the search.

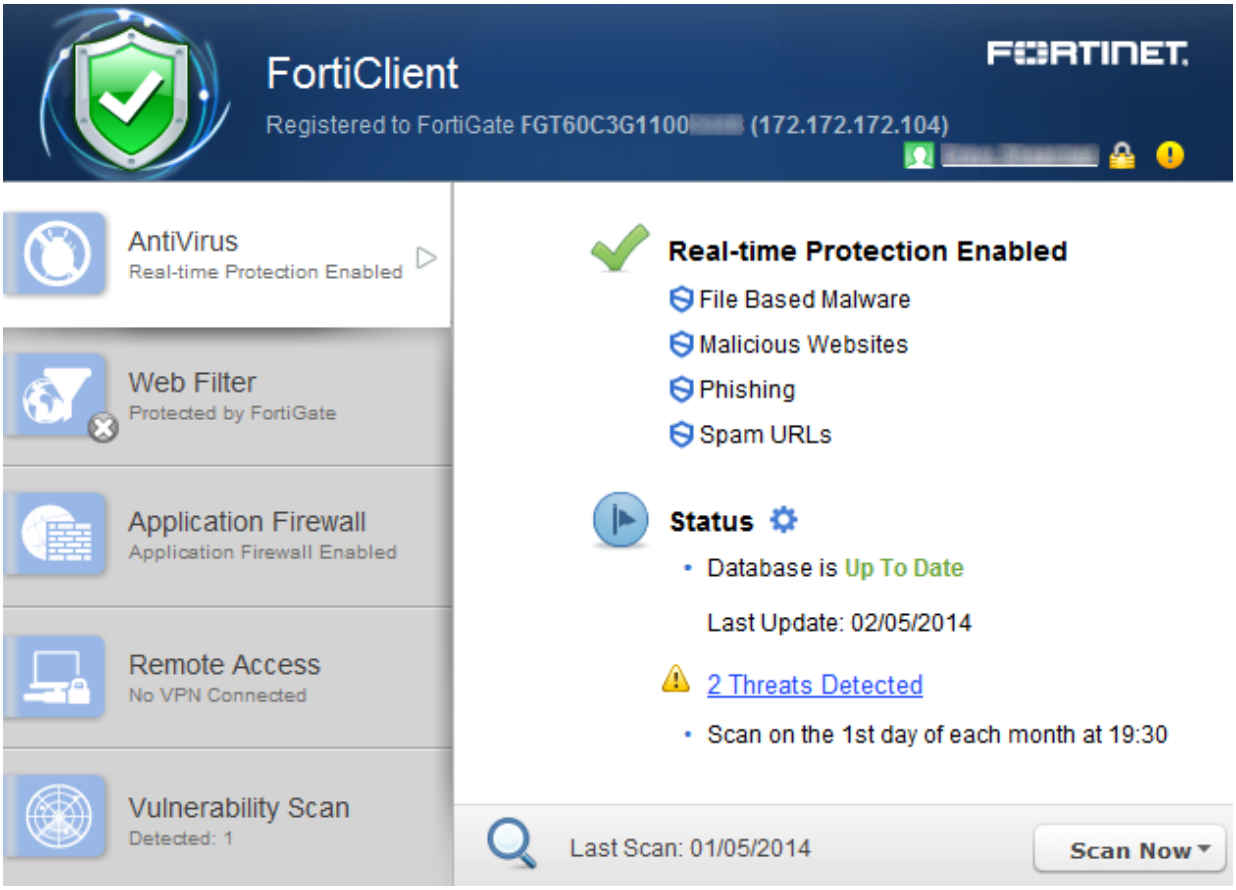
If FortiClient is unable to detect a FortiGate device, enter the IP address or URL of the device and select the *Go* icon. When FortiClient locates the FortiGate, you will be prompted to confirm the registration. Select the *Accept* button to complete registration. Upon successful registration, the FortiGate will send the FortiClient profile configuration.

3. Deploy the FortiClient profile from the FortiGate device.

   The FortiGate will deploy the FortiClient profile after registration is complete. This FortiClient profile will permit traffic through the FortiGate. A system tray bubble message will be displayed once update is complete.



The FortiClient console will display that it is successfully registered to the FortiGate. The FortiClient profile is installed on FortiClient.



Deploy the FortiClient profile to clients over a VPN connection:

1. In the FortiClient console, select the *Register to FortiGate* button. Enter the IP address and port number (if required) of the FortiGate's internal interface and select the *Go* icon.
2. Configure an IPsec VPN connection from FortiClient to the management FortiGate. For more information on configuring IPsec VPN see Create a new IPsec VPN connection on page 104.
3. Connect to the VPN.
4. You can now search for the FortiGate gateway. See Register FortiClient. on page 53 for more information.
5. After registration, the client is able to receive the FortiClient profile.

When creating a new FortiClient VPN (IPsec) or SSL VPN tunnel configuration on your FortiGate device, you must enable *Endpoint Registration*. See the *IPsec VPN for FortiOS* and *SSL VPN for FortiOS* sections of the *FortiOS Handbook* for more information.

Configuring endpoint registration over a VPN

FortiGate units can register FortiClient-equipped endpoints over either an interface-based IPsec VPN or a tunnel-mode SSL VPN. After the user authenticates, the FortiGate unit sends the FortiClient application the IP address

and port to be used for registration. If the user accepts the FortiGate invitation to register, registration proceeds and the FortiClient profile is downloaded to the client.

Users without FortiClient Endpoint Security connecting to the SSL VPN through a browser can be redirected to a captive portal to download and install the FortiClient software. The security policy must enable *Compliant with FortiClient Profile* and disable *Captive Portal Exempt*.

Endpoint registration on an IPsec VPN

You can enable endpoint registration when you configure the FortiClient VPN or you can enable it on an existing FortiClient VPN.

To enable endpoint registration while configuring the VPN:

Enable *Allow Endpoint Registration* on the *Network* page of the *VPN Wizard* when creating the FortiClient VPN.

To enable endpoint registration on an existing VPN:

1. Go to *System* > *Network* > *Interfaces* and edit the VPN's tunnel interface. The tunnel is a subinterface of the physical network interface.
2. In *Administrative Access*, make sure that *FCT-Access* is enabled.
3. Select *OK*.

Endpoint registration on the SSL VPN

To enable endpoint registration on the SSL VPN:

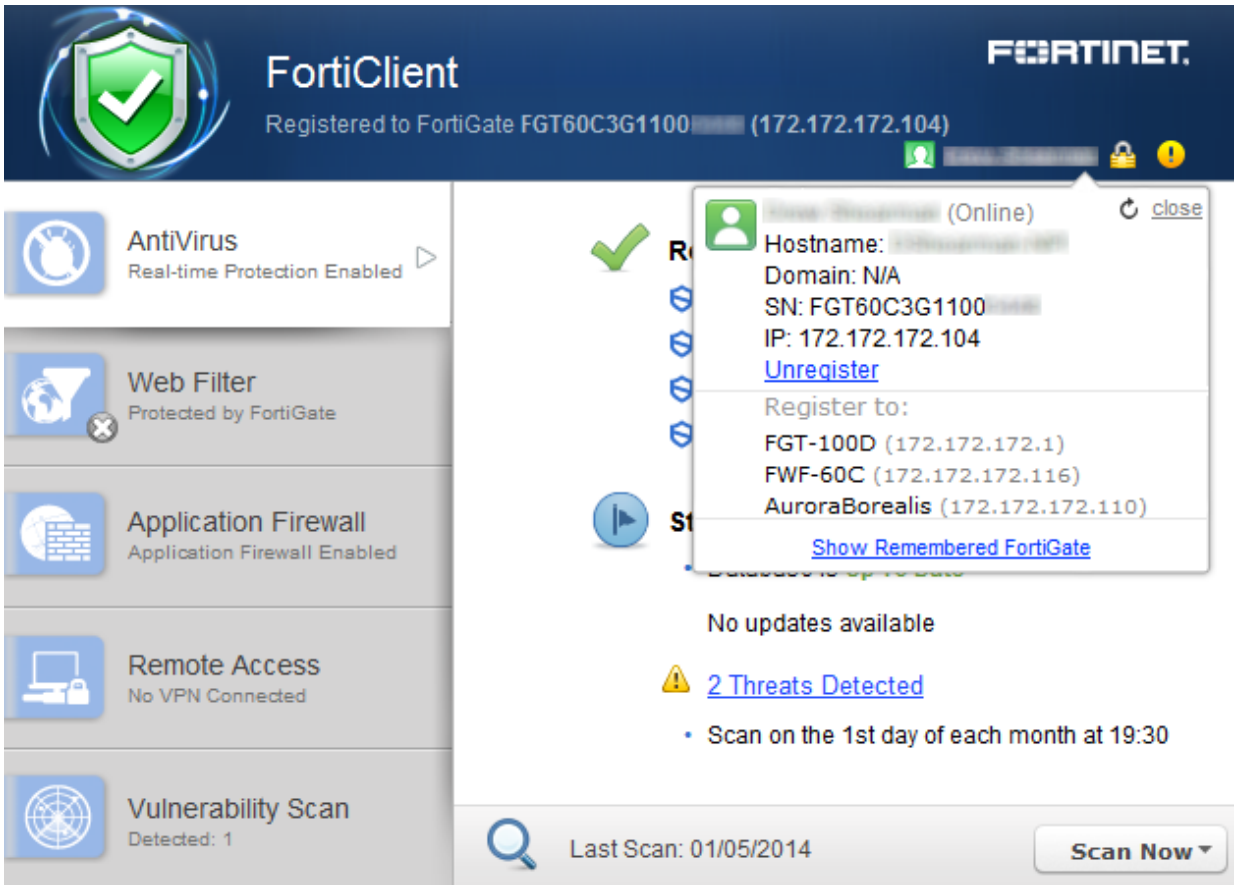
1. Go to *VPN* > *SSL* > *Portal*.
2. Make sure *Enable Tunnel Mode* is enabled.
3. Optionally, enable *Include FortiClient Download*.
   Users who access the VPN with a browser will be able to download FortiClient Endpoint Security for their device.
4. Select *Apply*.

Remembered FortiGates

FortiClient v5.0.1 or later adds the option to remember up to 20 FortiGate devices when accepting the broadcast registration message. FortiClient can remember and register to multiple FortiGate devices. This feature enables users to move freely between office locations and register conveniently to each FortiGate device.

When prompted to enter a registration key, FortiClient can remember the registration password.

Select the registration button in the console to view information for the current registered device including the IP address, serial number, endpoint user, domain, and hostname.



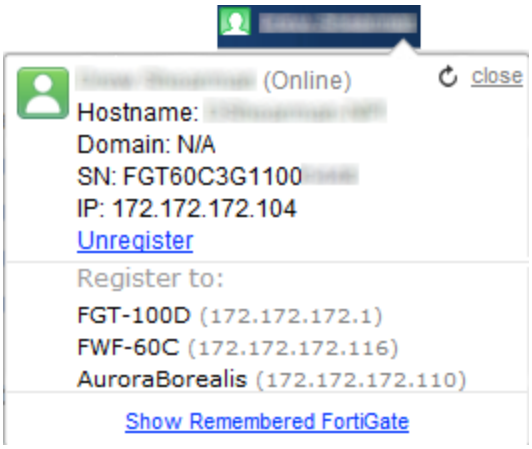
Forget a remembered FortiGate:

1. In the FortiClient console, click on the registered device name to display the registration dialog box.
2. Select *Show Remembered FortiGate* to show a list of FortiGate devices that FortiClient has previously registered with.
3. Select the device that you would like to remove from the remembered FortiGates list and select the *Forget* link.

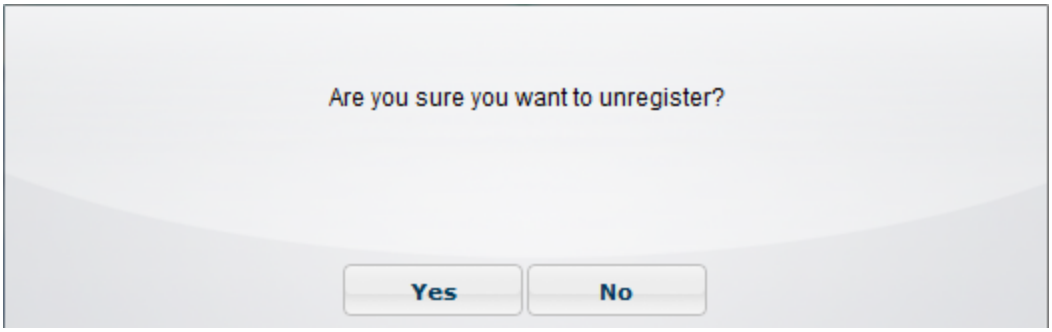
When selecting to forget a FortiGate, FortiClient will not automatically register to the FortiGate when re-connecting to the network. When the FortiGate is detected, you will be prompted to accept registration.

Unregister from FortiGate:

1. In the FortiClient console, click on the registered device name to display the registration details. The *Registration* dialog box appears.



2. Select *Unregister* in the registration dialog box. A confirmation dialog box is displayed.



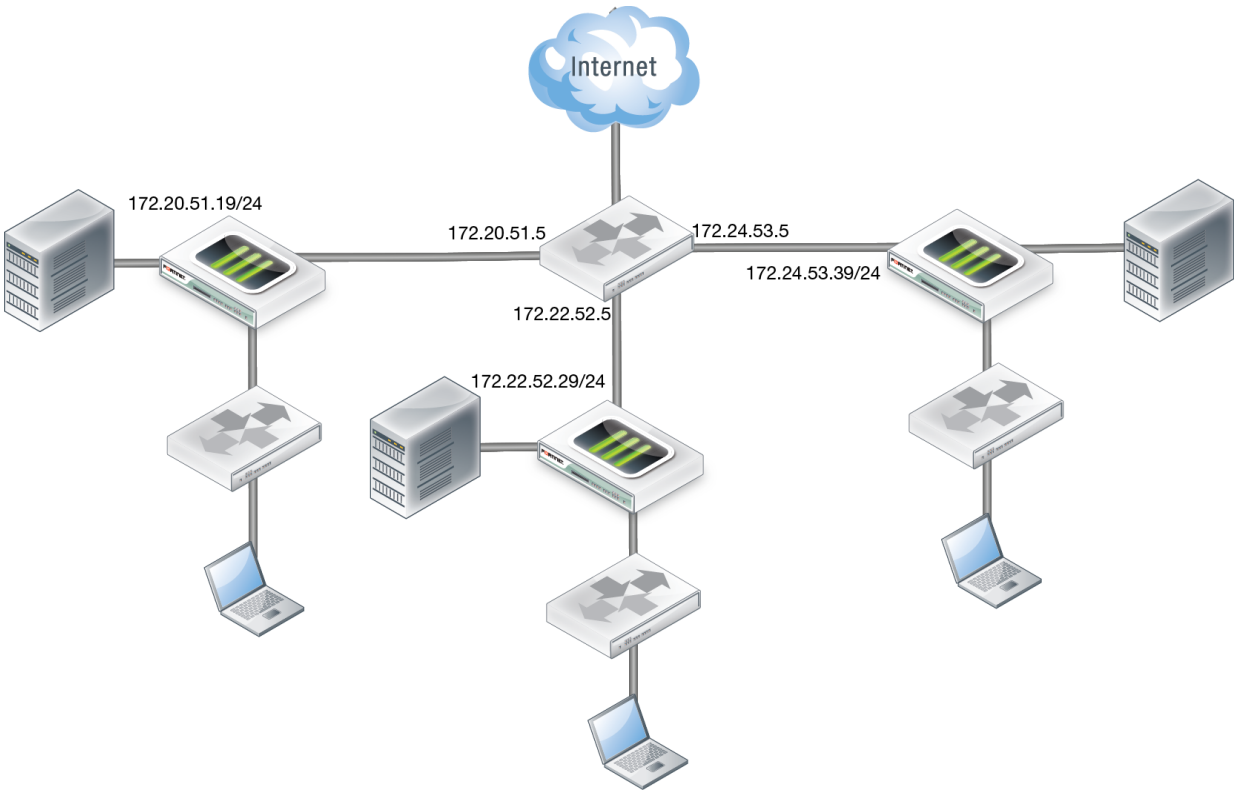
3. Select *Yes* to unregister FortiClient from the FortiGate selected.

When selecting to unregister from FortiGate, FortiClient will automatically register with the FortiGate when re-connecting to the network. To prevent this behavior, you must select to *Forget* the device.

Roaming clients (multiple redundant gateways) example

The following figure illustrates three corporate FortiGate networks. Each FortiGate can reach each other over a WAN network. FortiClient can only reach one FortiGate at a time. FortiClient may connect directly to the FortiGate or through a NAT device.

Roaming clients topology



If FortiClient connects through a NAT device to the FortiGate, do not enforce endpoint control compliance on the FortiGate.

On each of the three FortiGate devices configure the following:

- Interface IP addresses
- FortiClient profile
- Device identification in the interface
- FortiClient profile in the applicable firewall policy
- Endpoint control synchronization

Endpoint control synchronization allows you to synchronize endpoint control for multiple FortiGate devices. To enable endpoint control synchronization via the CLI enter the following commands on your FortiGate:

```
config endpoint-control forticlient-registration-sync
   edit 1
      set peer-ip 172.20.52.19
      next
      edit 2
      set peer-ip 172.22.53.29
   end
end
```

The IP addresses set for the `peer-ip` field are the WAN IP addresses for each of the FortiGate devices in the synchronization group.

You need to add the following XML configuration to FortiClient for this synchronization group. Modify the configuration file to add the following:

```
<forticlient_configuration>
   <endpoint_control>
      <!-- List of redundant FortiGates, since 5.0.2 -->
      <fortigates>
         <fortigate>
            <name>Corporate Network</name>
            <addresses>10.18.51.9;10.20.52.19;10.22.53.29</addresses>
         </fortigate>
      </fortigates>
   </endpoint_control>
</forticlient_configuration>
```

The IP addresses are the internal IP addresses for each of the three FortiGates in the synchronization group. FortiClient can reach any of these IPs, one at a time.

If the three FortiGate devices share the same DNS name, use the following XML configuration:

```
<forticlient_configuration>
   <endpoint_control>
      <!-- List of redundant FortiGates, since 5.0.2 -->
      <fortigates>
         <fortigate>
            <name>Fortinet Americas</name>
            <addresses>fct_americas.fortinet.com</addresses>
         </fortigate>
      </fortigates>
   </endpoint_control>
</forticlient_configuration>
```

The DNS server should return one reachable FortiGate IP address for the domain name used.

You will need to manually add FortiClient to the synchronization group when FortiClient initially registers with the FortiGate. Once added, no further action is required.

On your FortiGate, use the following CLI command to list all registered FortiClient endpoints:

```
diagnose endpoint registration list registered-forticlients
   FortiClient #1 (0):
   UID = BE6B76C509DB4CF3A8CB942AED200000
   vdom = root
   status = registered
   registering time = Fri May 2 15:00:07 2014
   registration expiry time = none
   source IP = 172.172.172.111
   source MAC = b0:ac:6f:70:e0:a0
   user = user
   host OS = Microsoft Windows 7 , 64-bit
   restored registration = no
   remote registration = yes
   registration FGT = FGT60C3G11000000
   Total number of licences: 10
   Total number of granted licenses: 1
   Total number of available licences: 9
```

The `remote registration` entry indicates whether this specific FortiClient is registered to this FortiGate, or to another FortiGate within the synchronization group.

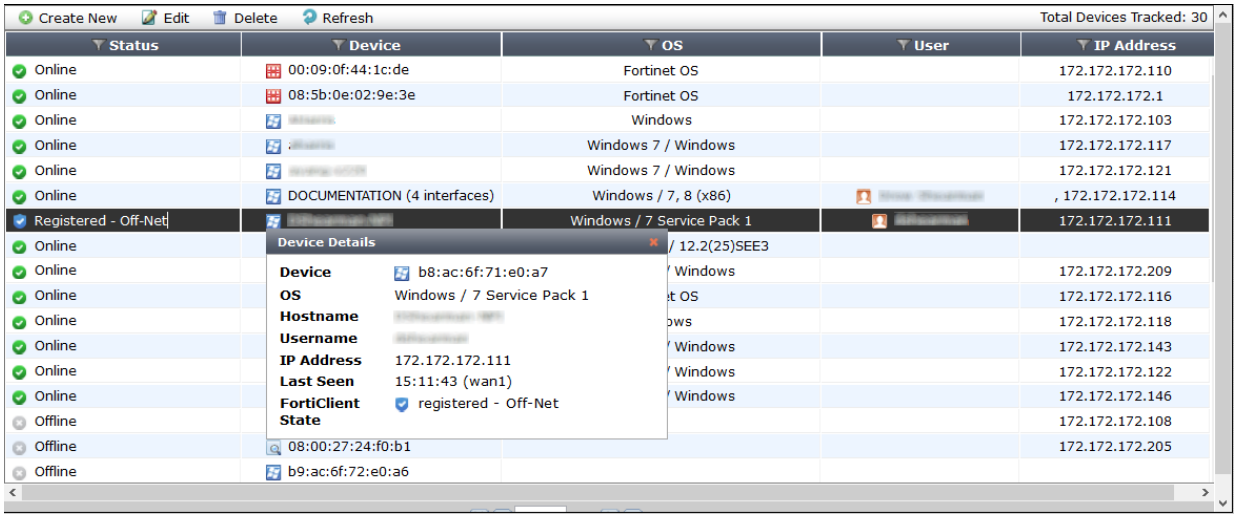
If any of the FortiGate devices require a password to complete registration, you can use the following XML configuration to provide password information to FortiClient:

```
<forticlient_configuration>
   <endpoint_control>
```

```
        <!-- List of redundant FortiGates, since 5.0.2 -->
        <fortigates>
           <fortigate>
              <name>Corporate Network</name>
              <addresses>10.18.51.9;10.20.52.19;10.22.53.29</addresses>
              <registration_password>uNbre@kab1e</registration_password>
           </fortigate>
        </fortigates>
     </endpoint_control>
</forticlient_configuration>
```

View FortiClient registration in the FortiGate GUI

You can view all registered FortiClient agents in the FortiGate GUI. Each new registration will be automatically added to the device table. To view registered devices go to *User & Devices* > *Device* > *Device Definitions*. The state for the new FortiClient registration is listed as *registered*. Alternatively, go to *User & Device* >*Monitor* > *FortiClient*.



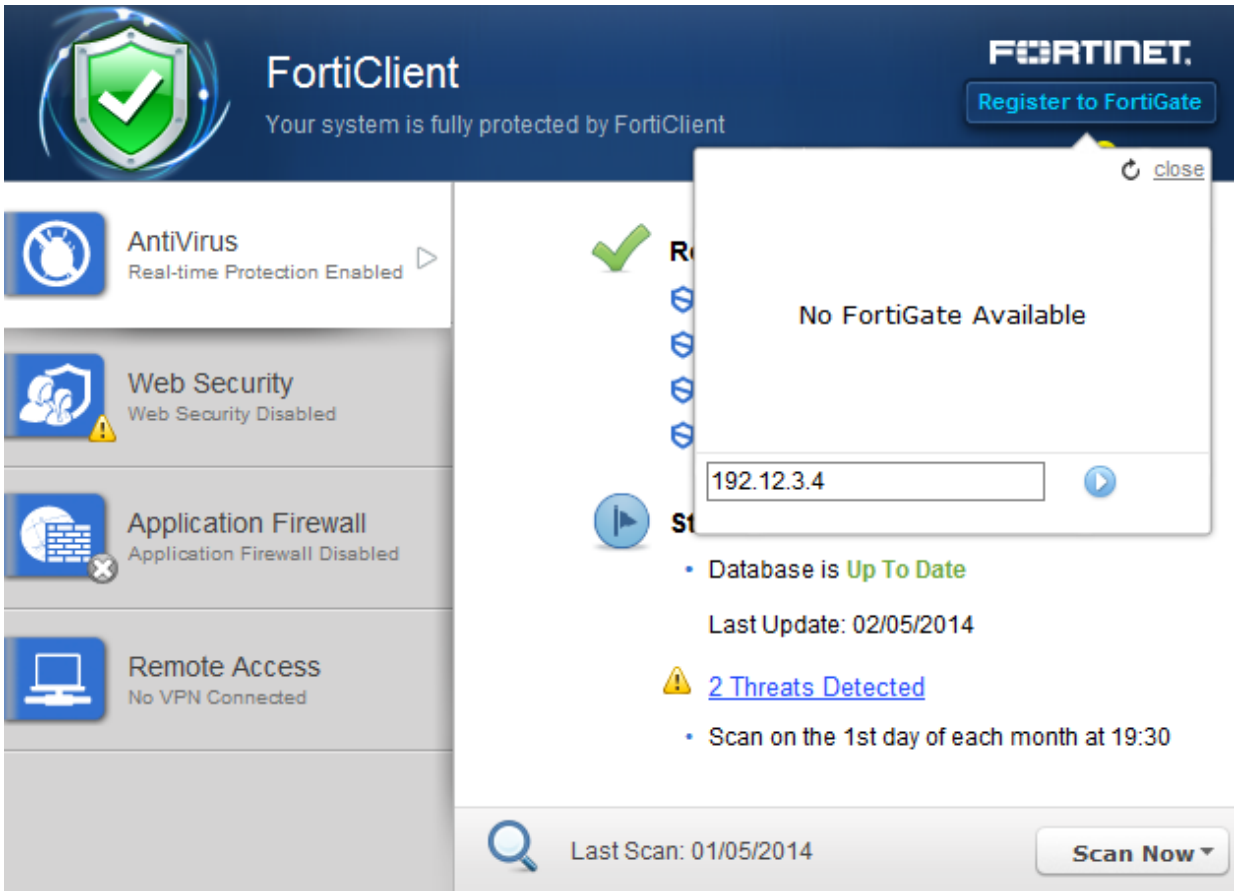
Configure the FortiGate IP address in FortiClient for registration

The FortiClient administrative user can specify a FortiGate IP address for registration and client configuration management. When an unregistered FortiClient starts up, FortiClient will list all reachable FortiGates for endpoint control registration in the registration drop-down list. The list will include any FortiGate that sends endpoint control broadcasts. Select the registration button in the FortiClient console to list discovered FortiGates. Any IP address provided in the *Settings* page under the *Registration* element is included in the list.

To configure a FortiGate IP address in FortiClient, select the *Register to FortiGate* button in the FortiClient console. In the *Specify Address* field, enter the IP address and port number (if required) of the FortiGate's internal interface, and select the *Go* icon.

Configure FortiGate in FortiClient

The FortiClient settings are locked, and cannot be modified after registration to a FortiGate is completed. See Configuration lock on page 135 for information on configuring this feature.

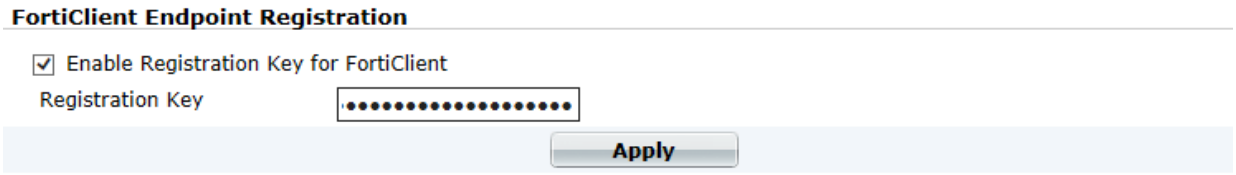


Enable FortiClient endpoint registration key password (optional)

You can configure a registration key password for FortiClient endpoint registration. Upon registering to FortiGate, the user will need to enter the registration key password before registration can be completed.

Enable registration key password requirement on registration:

1. On your FortiGate device, go to *System* > *Config* > *Advanced*.
2. Under *FortiClient Endpoint Registration*, select *Enable Registration Key for FortiClient* and enter a registration key password.



3. Select *Apply* to save the setting.

   Alternatively, you can configure this via the CLI. On your FortiGate device, go to S*ystem* > *Dashboard* > *Status*. Enter the following the CLI command in the *CLI Console* widget:

```
config endpoint-control settings
   set forticlient-key-enforce enable
   set forticlient-reg-key <password>
end
```

4. When FortiClient users attempt to register with FortiGate, they will receive the Registering to FortiGate dialog box. The user will need to enter the registration key password you configured before they can register to FortiGate.

FortiClient users can select to remember the registration key password in this page.

Display or hide the FortiClient profile details

You can select to display or hide the FortiClient profile details in the Registering to FortiGate page. When disabled, the user will not be able to view the profile details prior to completing registration to FortiGate.

To display or hide the FortiClient profile details:

1. On your FortiGate device, go to *System* > *Dashboard* > *Status*.
2. Enter the following the CLI command in the *CLI Console* widget:

```
config endpoint-control profile
   edit <profile name>
   config forticlient-winmac-settings
      set view-profile-details {enable | disable}
   end
end
```

Update FortiClient registration license on FortiGate

To update the FortiClient registration license on FortiGate, use the following CLI command:

```
execute FortiClient-NAC update-registration-license <license key/activation code>
```

Endpoint registration with Active Directory (AD) user groups

The user's AD domain name and group are both sent to the FortiGate during endpoint registration. Administrators may configure the FortiGate to deploy endpoint and/or firewall profiles based on the end user's AD domain group. This feature requires FortiClient v5.0.4 or later and FortiOS v5.0.3 or later.

The following steps are discussed in more details:

Configure users and groups on your AD server

Create the user accounts and groups on the AD server. Groups may have any number of users. A user may belong to more than one group at the same time.

Configure your FortiAuthenticator

Configure FortiAuthenticator to use the AD server that you created. For more information see the *FortiAuthenticator v3.0 Administration Guide*.

Configure your FortiGate

Configure FortiGate from the GUI as listed below.

Add the FortiAuthenticator or Fortinet Single Sign-On Agent (FSSO):

1. Go to *User & Device* > *Authentication* > *Single Sign-On*.
2. Select *Create New* in the toolbar. The *New Single Sign-On Server* window opens.

3. In the type field, select *Fortinet Single-Sign-On Agent*.
4. Enter the information required for the agent. This includes the name, primary and secondary IP address and password. Select an LDAP server in the drop-down list if applicable. Select *More FSSO agents* to add up to three additional agents.
5. Select *OK* to save the agent configuration.

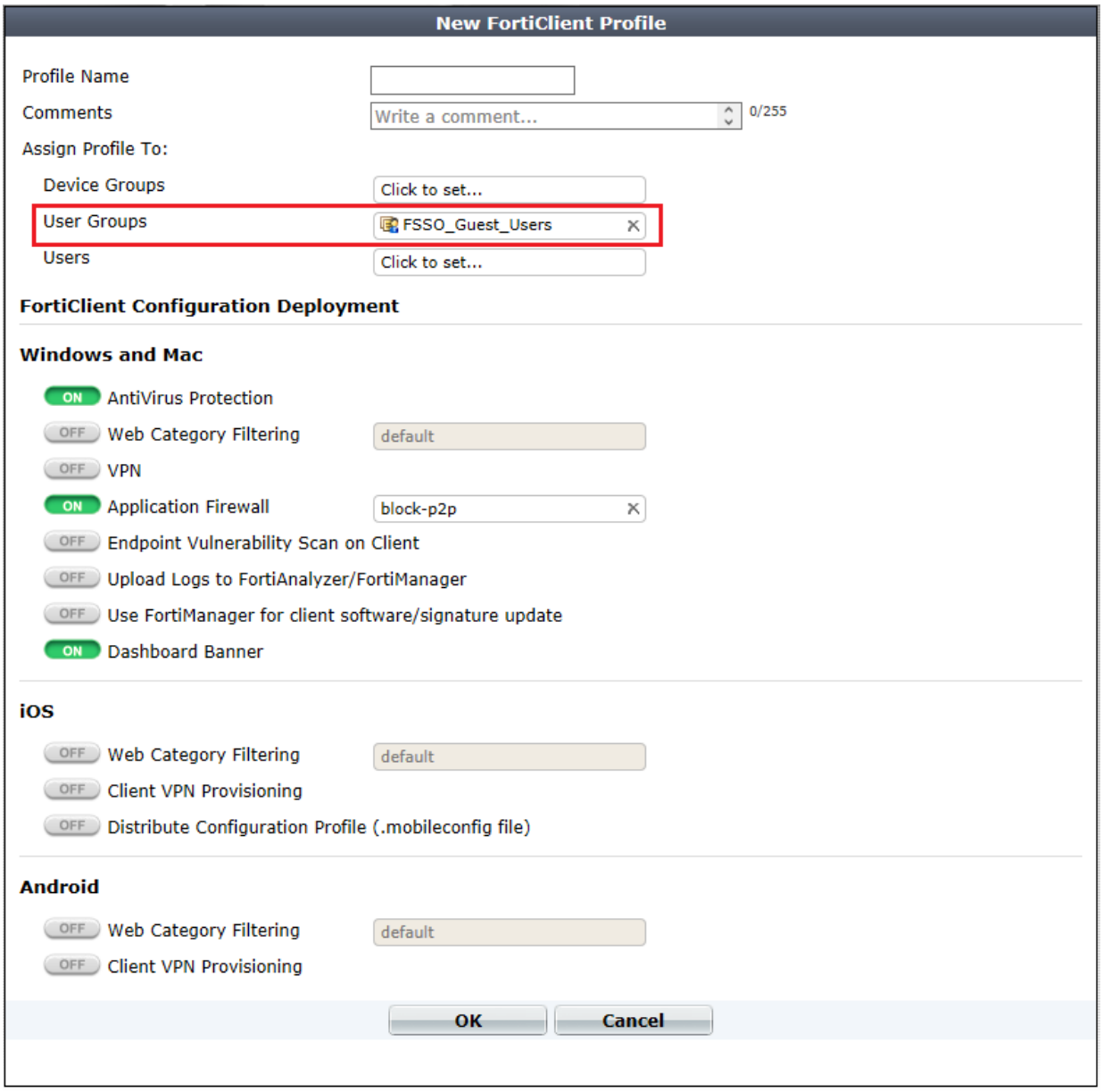
Create a user group:

1. Go to *User & Device* > *User* > *User Groups*.
2. Select *Create New* in the toolbar. The *New User Group* window opens.

3. In the type field, select *Fortinet Single-Sign-On (FSSO)*.
4. Select members from the drop-down list.
5. Select *OK* to save the group configuration.

Configure the FortiClient profile:

1. Go to *User & Device* > *FortiClient Profiles*.
2. Select *Create New* in the toolbar. The *New FortiClient Profile* window opens.



3. Enter a profile name and optional comments.
4. In the *User Groups* drop-down list select the FSSO user group(s).
5. Configure FortiClient configuration deployment as required.
6. Select *OK* to save the new FortiClient profile.

   For more information see Configure endpoint management on page 43.

Create any number of FortiClient profiles with different groups and different settings. The default profile will be assigned to users who register successfully but have no matching FortiClient profile.

Configure the firewall policy:

Configure the firewall policy as described in Configure endpoint management on page 43. Ensure that *Compliant with FortiClient Profile* is selected in the policy.

Connect to the FortiGate using FortiClient endpoint

The Microsoft Windows system on which FortiClient is installed should join the domain of the AD server configured earlier. Users may login with their domain user name.

Following this, FortiClient endpoint registrations will send the logged-in user's name and domain to the FortiGate. The FortiGate will assign the appropriate profiles based on the configurations.

Monitoring client registrations

The following FortiOS CLI command lists information about registered clients. This includes domain-related details for the client (if any).

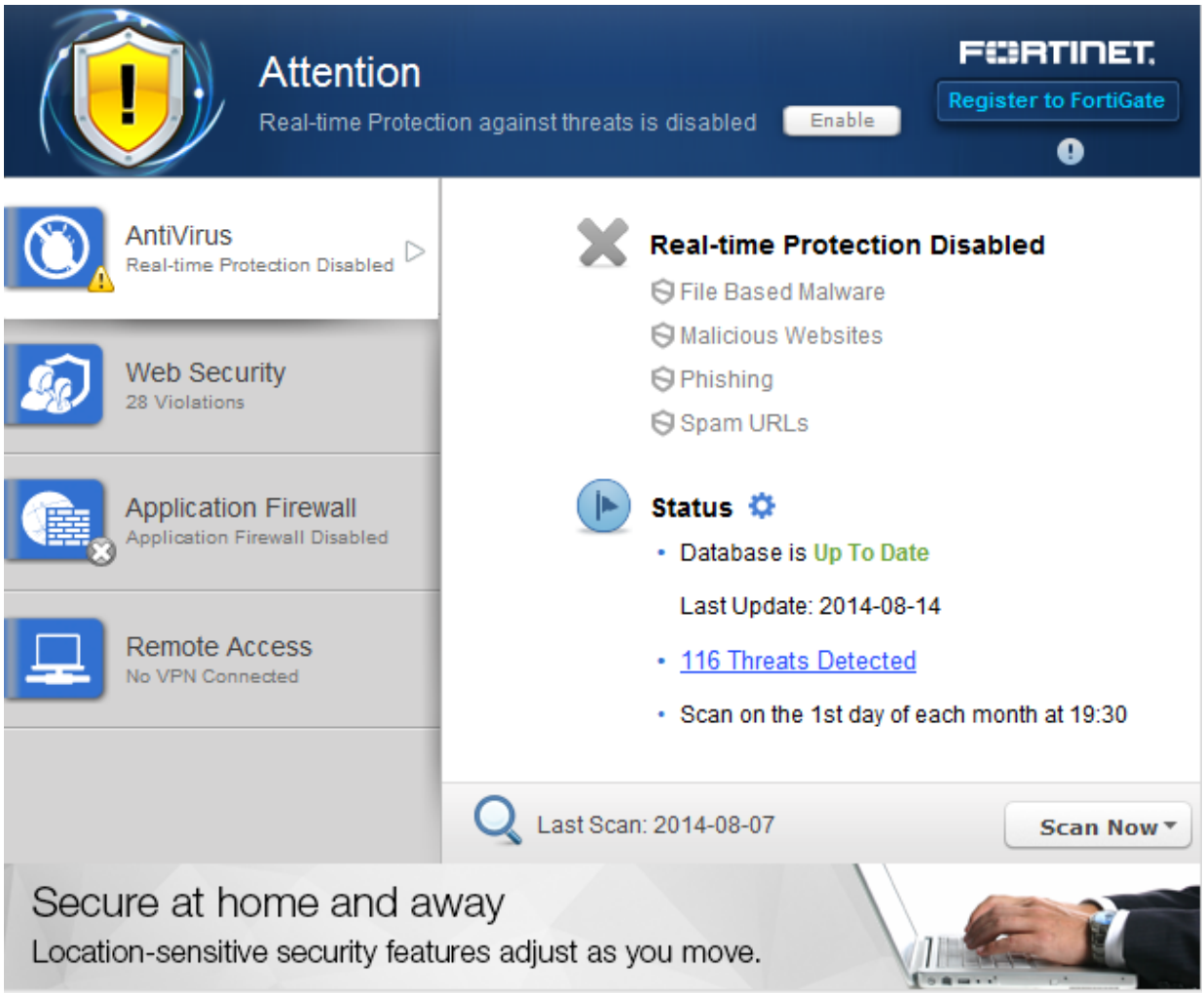
```
diagnose endpoint record-list
   Record #1:
      IP_Address = 172.172.172.111(1)
      MAC_Address = b0:ac:6f:70:e0:a0
      Host MAC_Address = b0:ac:6f:70:e0:a0
      MAC list = b0-ac-6f-70-e0-a0;
      VDOM = root
      Registration status: Forticlient installed but not registered
      Online status: offline
      DHCP on-net status: off-net
      DHCP server: None
      FCC connection handle: 6
      FortiClient version: 5.1.29
      AVDB version: 22.137
      FortiClient app signature version: 3.0
      FortiClient vulnerability scan engine version: 1.258
      FortiClient feature version status: 0
      FortiClient UID: BE6B76C509DB4CF3A8CB942AED2064A0 (0)
      FortiClient config dirty: 1:1:1
      FortiClient KA interval dirty: 0
      FortiClient Full KA interval dirty: 0
      FortiClient server config: d9f86534f03fbed109676ee49f6cfc09::
      FortiClient config: 1
      FortiClient iOS server mconf:
      FortiClient iOS mconf:
      FortiClient iOS server ipsec_vpn mconf:
      FortiClient iOS ipsec_vpn mconf:
      Endpoint Profile: Documentation
      Reg record pos: 0
      Auth_AD_groups:
      Auth_group:
      Auth_user:
      Host_Name:
      OS_Version: Microsoft Windows 7 , 64-bit Service Pack 1 (build 7601)
      Host_Description: AT/AT COMPATIBLE
      Domain:
      Last_Login_User: FortiClient_User_Name
      Host_Model: Studio 1558
```

```
Host_Manufacturer: Dell Inc.
CPU_Model: Intel(R) Core(TM) i7 CPU Q 720 @ 1.60GHz
Memory_Size: 6144
Installed features: 55
Enabled features: 21
online records: 0; offline records: 1
status -- none: 0; uninstalled: 0; unregistered: 1; registered: 0; blocked: 0
```

Antivirus

FortiClient Antivirus

FortiClient v5.2 includes an antivirus module to scan system files, executable files, removable media, dynamic-link library (DLL) files, and drivers. FortiClient will also scan for and remove rootkits. In FortiClient v5.2, File Based Malware, Malicious Websites, Phishing, and Spam URL protection is part of the antivirus module.



This section describes how to enable antivirus and configuration options.

Enable or disable antivirus

To enable FortiClient antivirus real-time protection, select the enable icon in the FortiClient console. To disable FortiClient antivirus real-time protection, select the disable link beside *Real-time Protection Enabled* in the FortiClient console.

When FortiClient is registered to FortiGate for endpoint control, antivirus is enabled and disabled in the FortiClient Profile.

If you have another antivirus program installed on your system, FortiClient will prompt the following dialog box warning that your system may lock up due to conflicts between different antivirus products.

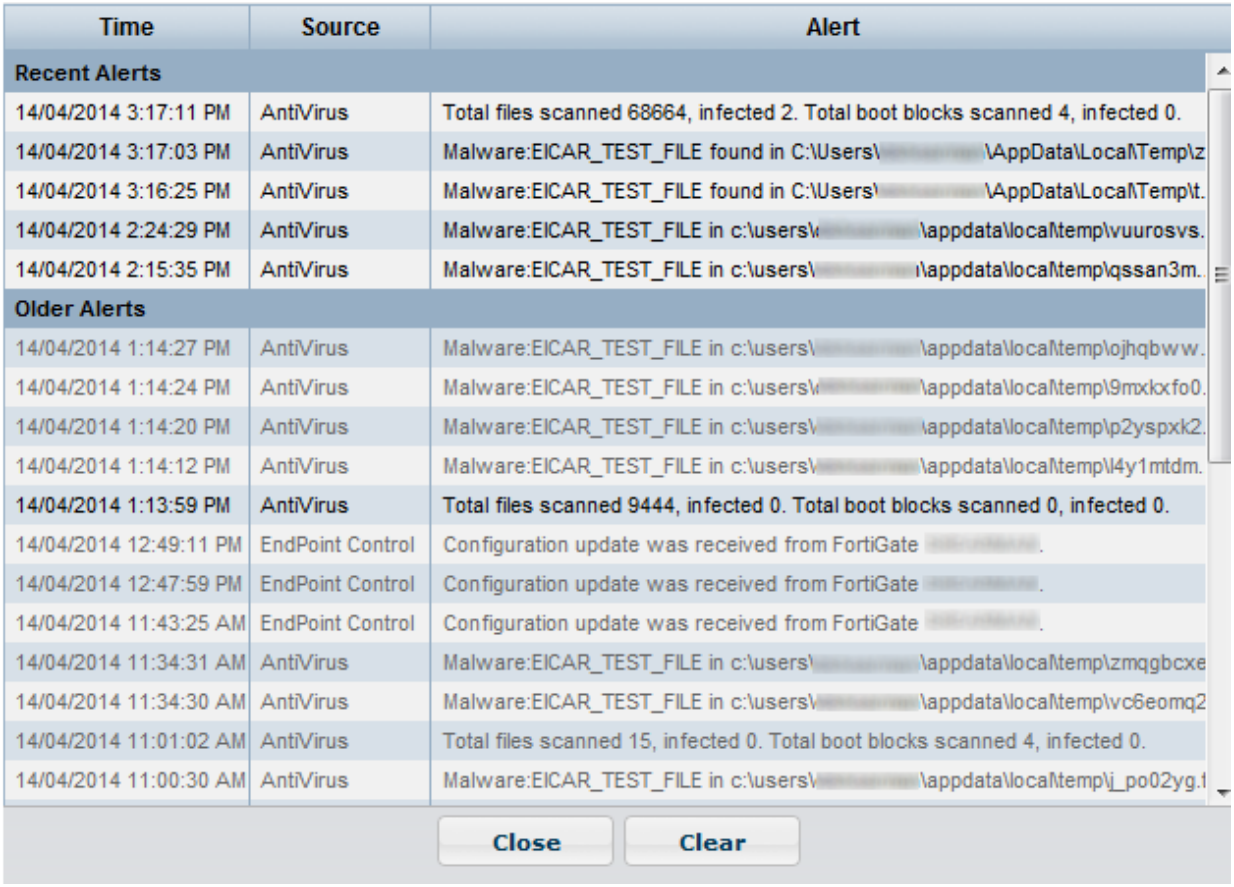
It is recommended to remove the conflicting antivirus product before installing FortiClient or enabling the antivirus real-time protection feature.

Notifications

Select the notifications icon in the FortiClient console to view all notifications. When a virus has been detected, the notifications icon will change from gray to yellow.

Select *View All* in the drop-down *Notifications* window to view all event notifications. Event notifications include:

- AntiVirus events including scheduled scans and detected malware.
- Endpoint Control events including configuration updates received from FortiGate.
- WebFilter events including blocked web site access attempts.
- System events including signature and engine updates and software upgrades.



Select the Threat Detected link to view quarantined files, site violations, and real-time protection events.

Scan now

To perform on-demand antivirus scanning, select the *Scan Now* button in the FortiClient console. Use the drop-menu to select *Custom Scan, Full Scan*, *Quick Scan*, or *Removable media Scan*. The console displays the date of the last scan to the left of the button.

- *Custom Scan* runs the rootkit detection engine to detect and remove rootkits. *Custom Scan* allows you to select a specific file folder on your local hard disk drive (HDD) to scan for threats.
- *Full Scan* runs the rootkit detection engine to detect and remove rootkits. *Full Scan* then performs a full system scan including all files, executable files, DLLs, and drivers for threats.
- *Quick System Scan* runs the rootkit detection engine to detect and remove rootkits. *Quick System Scan* only scans executable files, DLLs, drivers that are currently running for threats.
- *Removable media Scan* runs the rootkit detection engine to detect and remove rootkits. *Removed media Scan* scans all connected removable media such as USB drives.

Scan a file or folder on your workstation

To perform a virus scan a specific file or folder on your workstation, right-click the file or folder and select *Scan with FortiClient AntiVirus* from the menu.

Submit a file for analysis

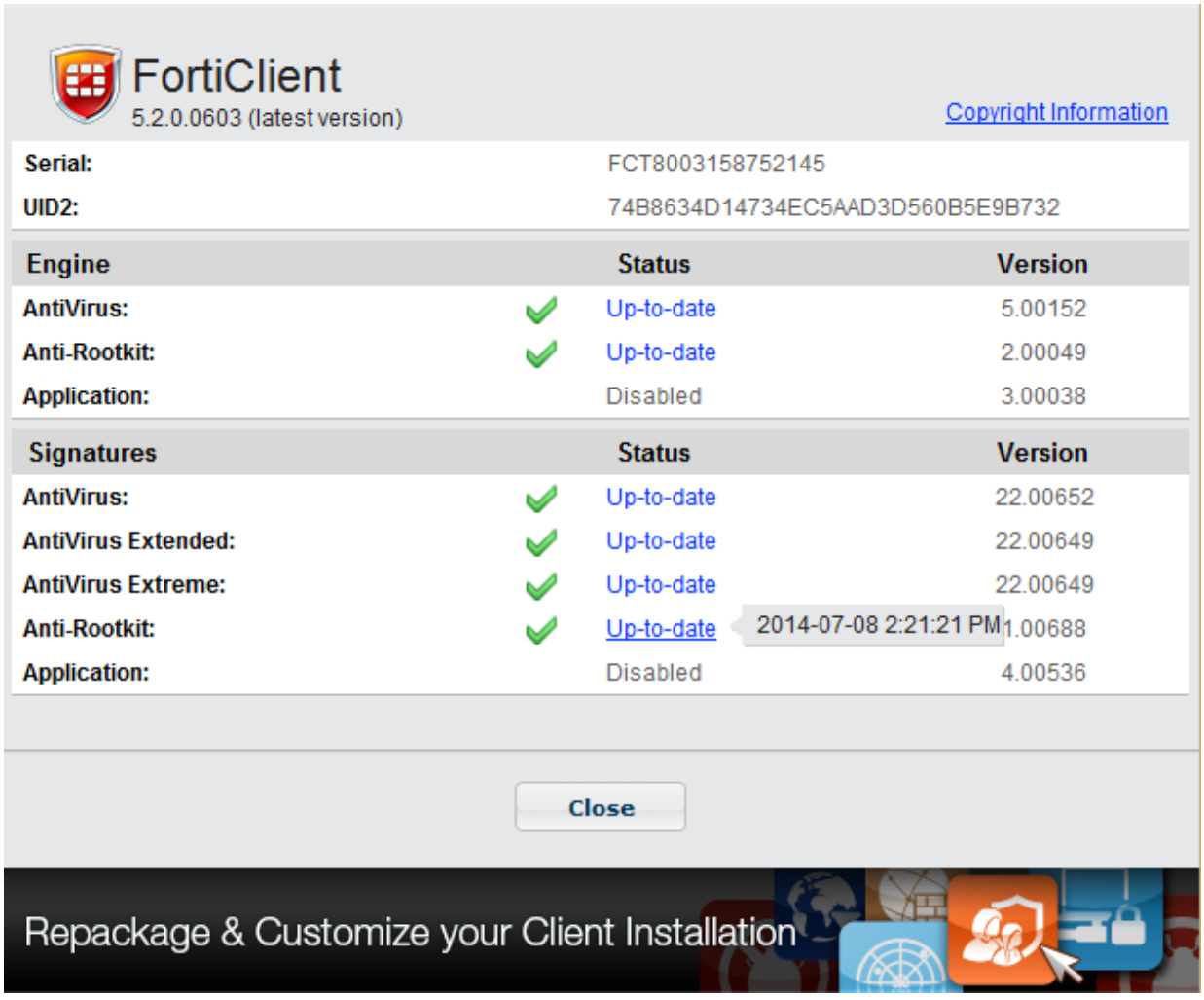
You can select to send up to 5 files a day to FortiGuard for analysis. To submit a file, right-click a file or executable and select Submit for analysis from the menu. A dialog box will be displayed which allows you to see the number of files you have submitted. Confirm the file location of the file you want to submit and select the *Submit* button.

You do not receive feedback for files submitted for analysis. The FortiGuard team is able to create signatures for any files which are submitted for analysis and determined to be malicious.

View FortiClient engine and signature versions

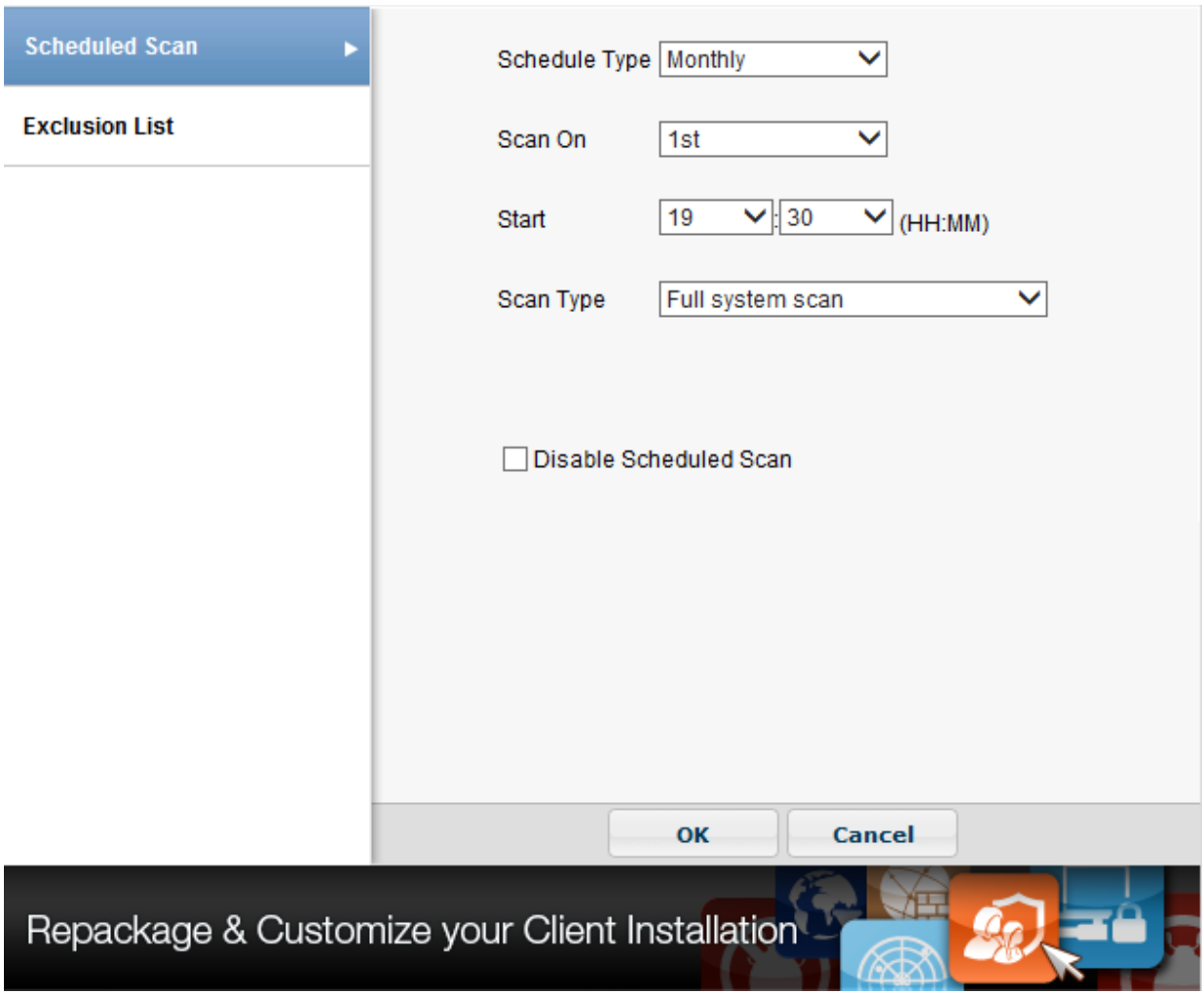
To view the current FortiClient version, engine, and signature information, select *Help* in the toolbar, and select *About* in the drop-down menu. Hover the mouse over the status field to see the date and time that FortiClient last updated the selected item.

When FortiClient is registered to FortiGate for endpoint control, you can select to use a FortiManager device for client software and signature updates. When configuring the FortiClient profile, select *Use FortiManager for client software/signature updates* to enable the feature and enter the IP address of your FortiManager device. You can select to failover to FDN when FortiManager is not available.



Schedule antivirus scanning

Select the settings icon beside *Status* in the FortiClient console to open the antivirus settings page. To schedule antivirus scanning, select the *Scheduled Scan* tab in the left pane.



Configure the following settings:

Schedule Type	Select Daily, Weekly or Monthly in the drop-down list.
Scan On	For Weekly scheduled scan, select the day of the week in the drop-down list. For Monthly scheduled scan, select the day of the month in the drop-down list.
Start	Select the start time in the drop-down lists. The time format is represented in hours and minutes, 24-hour clock.

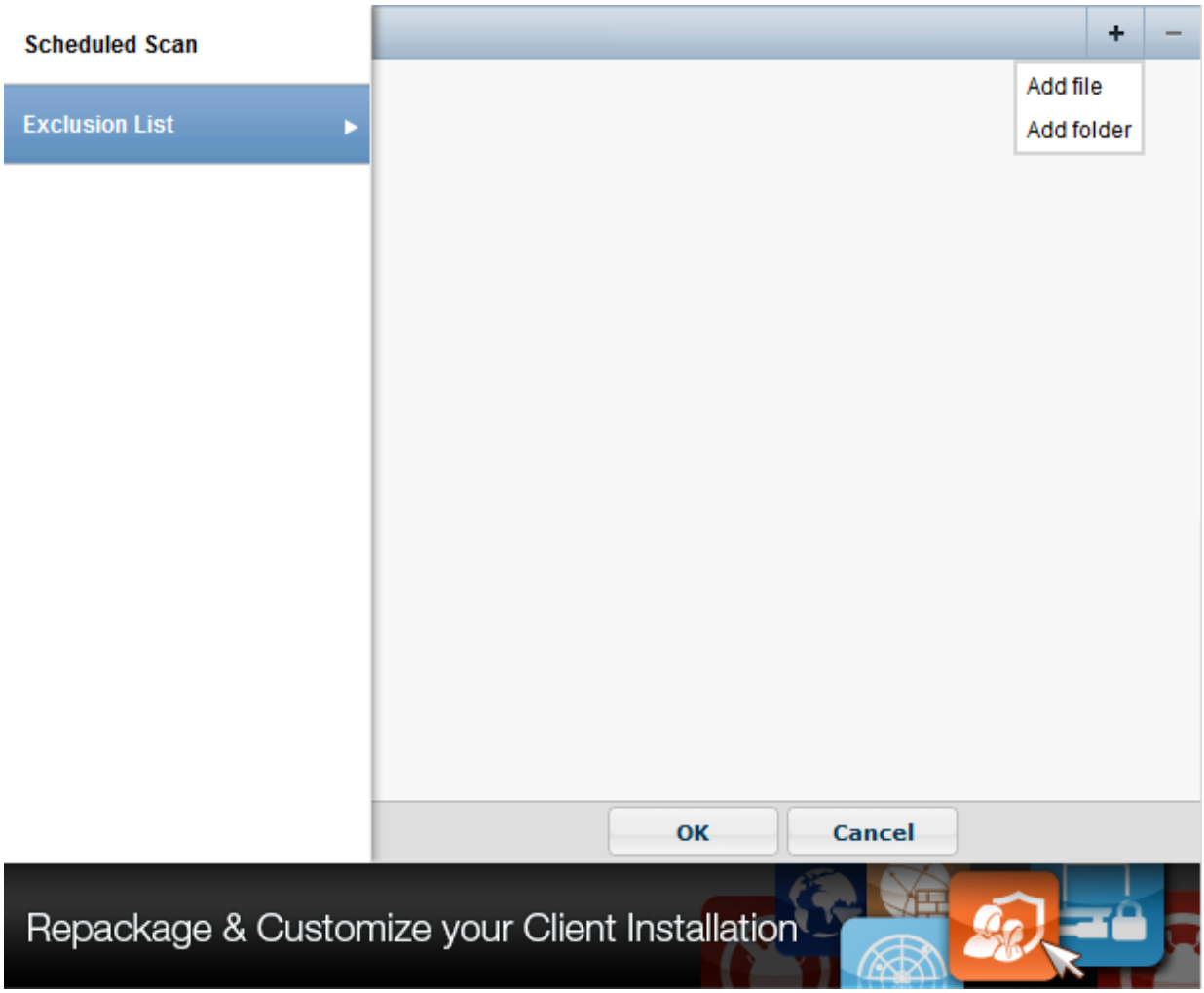
Scan Type	Select the scan type: • Custom Scan runs the rootkit detection engine to detect and remove rootkits. Custom Scan allows you to select a specific file folder on your local hard disk drive (HDD) to scan for threats. • Full Scan runs the rootkit detection engine to detect and remove rootkits. Full Scan then performs a full system scan including all files, executable files, DLLs, and drivers for threats. • Quick System Scan runs the rootkit detection engine to detect and remove rootkits. *Quick System Scan* only scans executable files, DLLs, drivers that are currently running for threats. You can schedule a removable media scan. A full scan will scan removable media.
Disable Scheduled Scan	Select to disable scheduled scan.

Select *OK* to save the setting and return to the main FortiClient console page.

If you configure monthly scans to occur on the 31st of each month, the scan will occur on the first day of the month for those months with less than 31 days.

Add files/folders to an exclusion list

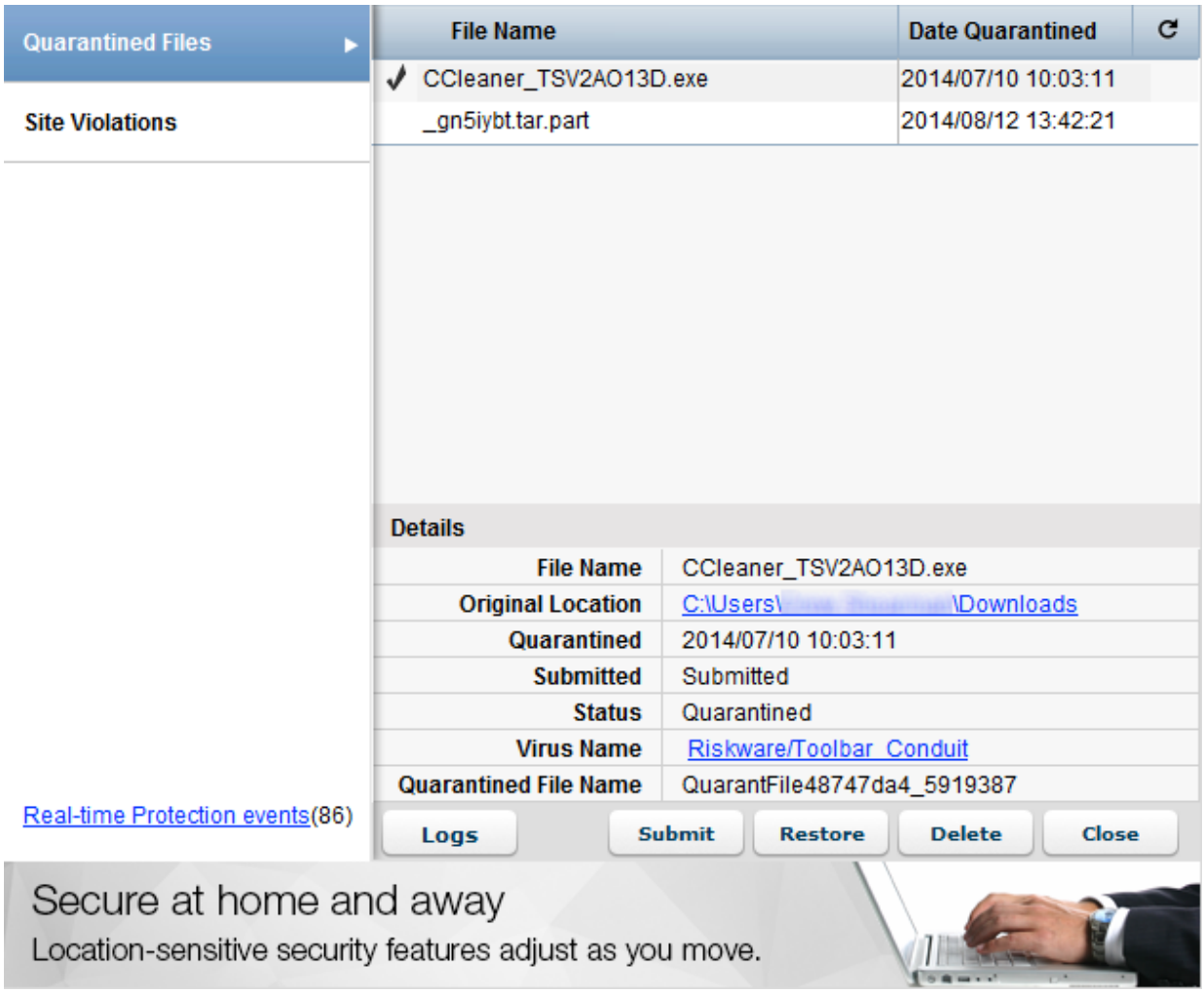
Select the settings icon beside *Status* in the FortiClient console to open the antivirus settings page. To create an exclusion list, select the *Exclusion List* tab in the left pane. To add files/folders to the antivirus exclusion list, select *Exclusion List* in the content pane. Select the add icon and then select Add file or Add folder from the drop-down list. Any files or folders in this exclusion list will not be scanned. Select the minus icon to remove files or folders from the list.



Select *OK* to save the setting and return to the FortiClient console page.

View quarantined threats

To view quarantined threats, select the *Threats Detected* link in the FortiClient console, and select *Quarantined Files* in the left tree menu. In this page you can view, restore, or delete the quarantined file. You can also view the original file location, the virus name, submit the suspicious file to FortiGuard, and view logs.



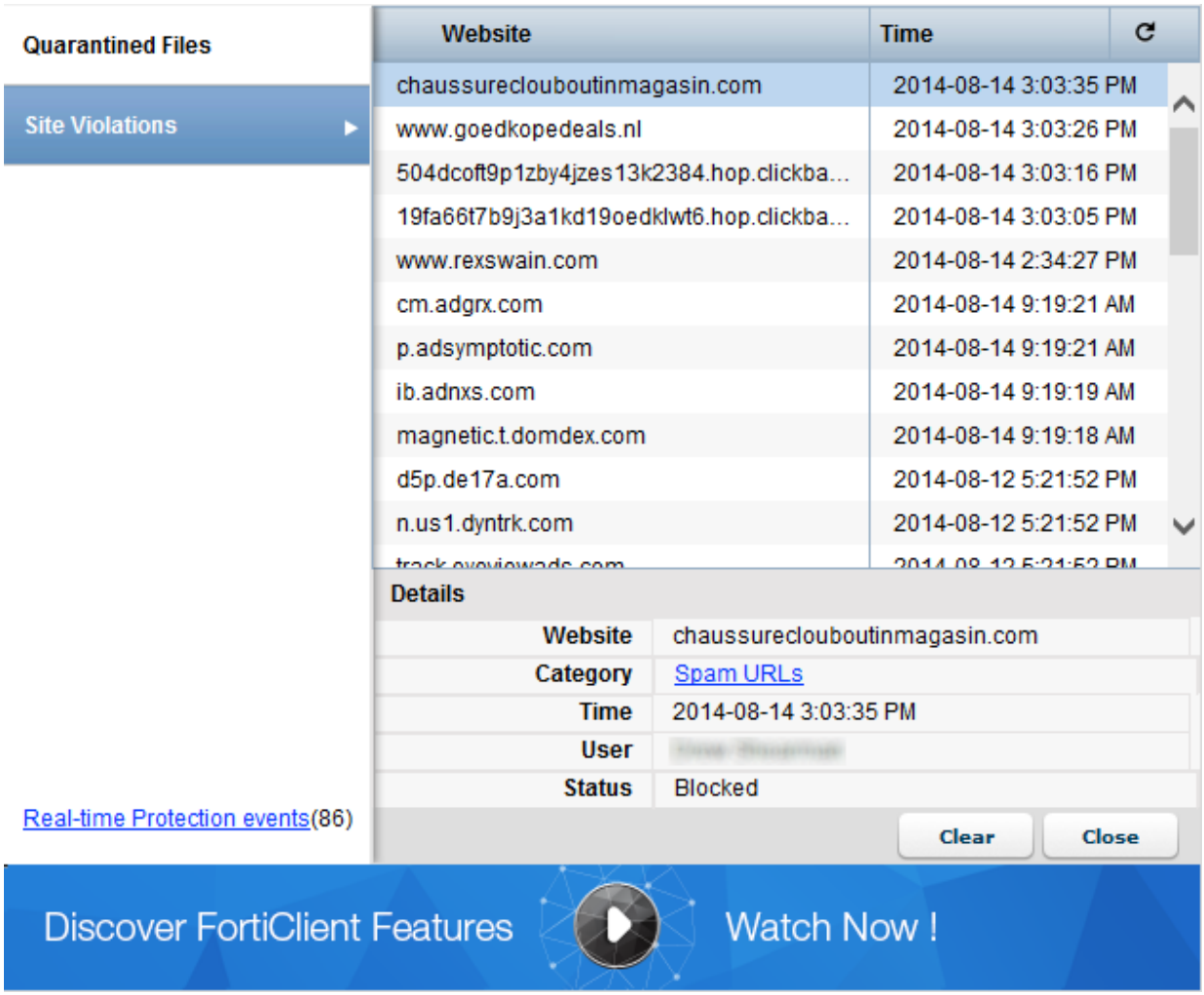
This page displays the following:

File Name	The name of the file.
Date Quarantined	The date and time that the file was quarantined by FortiClient.
Refresh	Select to refresh the quarantined files list.
Details	Select a file from the list to view detailed information including the file name, original location, date and time that the virus was quarantined, the submitted status, status, virus name, and quarantined file name.
Logs	Select to view FortiClient log data.
Refresh	Select to refresh the list.
Submit	Select to submit the quarantined file to FortiGuard. Press and hold the control key to submit multiple entries.

Restore	Select to restore the quarantined file. A confirmation dialog box will be displayed. You can select *Yes* to add this file/folder to the exclusion list, *No* to restore the file, or *Cancel* to exit the operation. Press and hold the control key to restore multiple entries.
Delete	Select to delete the quarantined file. A confirmation dialog box will be displayed, select *Yes* to continue. Press and hold the control key to delete multiple entries.
Close	Select to close the page and return to the FortiClient console.

View site violations

To view site violations, select the *Threats Detected* link in the FortiClient console, and select *Site Violations* in the left tree menu. In this page you can view site violations and submit sits to be re-categorized.

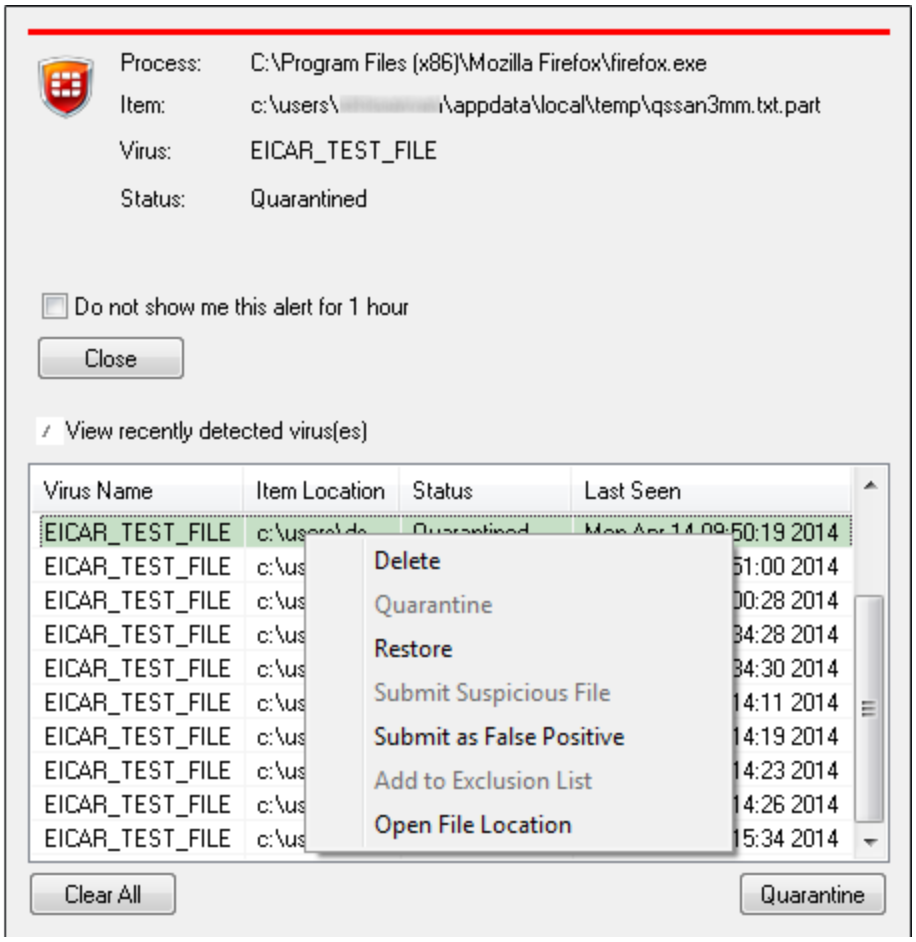


This page displays the following:

Website	Displays the name of the website.
Time	Displays the date and time of the site violation.
Refresh	Select to refresh the site violation list.
Details	Select an entry in the list to view site violation details including the website name, category, date and time, user name, and status. Select the category link to request to have the site category re-evaluated.

View alerts dialog box

When FortiClient antivirus detects a virus while attempting to download a file via a web-browser, you will receive a warning dialog message.



Select *View recently detected virus(es)* to collapse the virus list. Select a file in the list and right-click to access the context menu.

Delete	Select to delete a quarantined or restored file.
Quarantine	Select to quarantine a restored file.
Restore	Select to restore a quarantined file.
Submit Suspicious File	Select to submit a file to FortiGuard as a suspicious file.
Submit as False Positive	Select to submit a quarantined file to FortiGuard as a false positive.
Add to Exclusion List	Select to add a restored file to the exclusion list. Any files in the exclusion list will not be scanned.
Open File Location	Select to open the file location on your workstation.

When *Alert when viruses are detected* under *AntiVirus Options* is not selected, you will not receive the virus alert dialog box when attempting to download a virus in a web browser.

Real-time Protection events

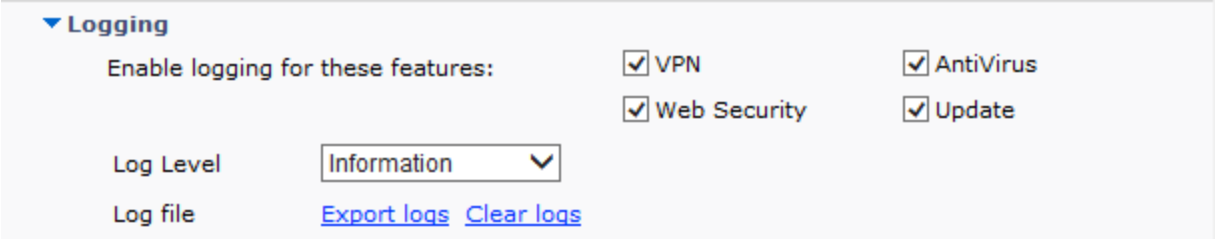
When an antivirus real-time protection event has occurred you can select to view these events in the FortiClient console. Select *AntiVirus* > *Threats Detected* and select *Real-time Protection events* in the left pane. The `realtime_scan.log` will open in the default viewer.

Example log output:

```
Realtime scan result:
time: 03/18/14 10:46:07, virus found: EICAR_TEST_FILE, action: Quarantined,
    c:\users\user\desktop\eicar.com
time: 03/18/14 10:46:07, virus found: EICAR_TEST_FILE, action: Quarantined,
    c:\users\user\desktop\eicar.com.txt
time: 03/18/14 10:46:07, virus found: EICAR_TEST_FILE, action: Quarantined,
    c:\users\user\desktop\eicarcom2.zip
time: 03/18/14 10:46:08, virus found: EICAR_TEST_FILE, action: Quarantined,
    c:\users\user\desktop\eicar_com.zip
time: 03/18/14 10:46:39, virus found: EICAR_TEST_FILE, action: Quarantined,
    c:\users\user\appdata\local\temp\3g_bl8y9.com.part
time: 03/18/14 10:48:13, virus found: EICAR_TEST_FILE, action: Quarantined,
    c:\users\user\appdata\local\temp\xntwh8q1.zip.part
```

Antivirus logging

To configure antivirus logging, select *File* in the toolbar and *Settings* in the drop-down menu. Select *Logging* to view the drop-down menu.

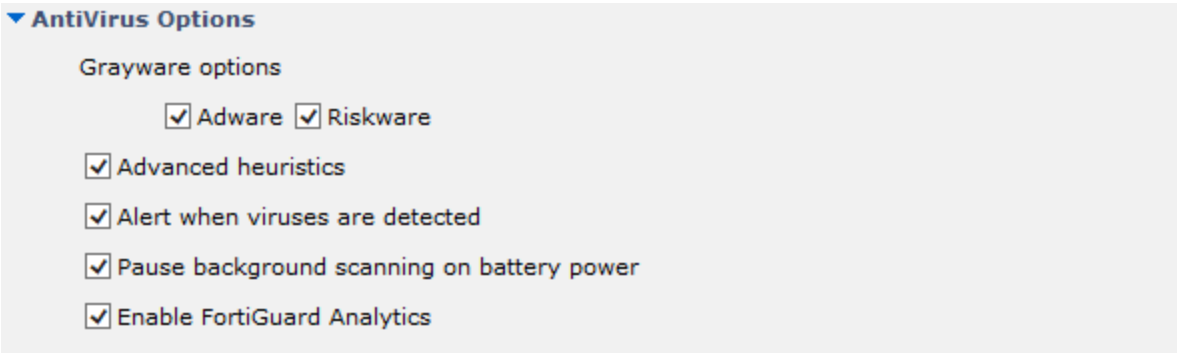


Configure the following settings:

Enable logging for these features	Select antivirus to enable logging for this feature.
Log Level	Select the level of logging: • Emergency: The system becomes unstable. • Alert: Immediate action is required. • Critical: Functionality is affected. • Error: An error condition exists and functionality could be affected. • Warning: Functionality could be affected. • Notice: Information about normal events. • Information: General information about system operations. • Debug: Debug FortiClient.
Log file	
Export logs	Select to export logs to your local hard disk drive (HDD) in `.log` format.
Clear logs	Select to clear all logs. You will be presented a confirmation window, select *Yes* to proceed.

Antivirus options

To configure antivirus options, select *File* in the toolbar, and *Settings* in the drop-down menu. Select *AntiVirus Options* to view the drop-down menu. In this menu you can configure options outlined in the following figure and table.



Configure the following settings:

Antivirus Options	
Grayware Options	Grayware is an umbrella term applied to a wide range of malicious applications such as spyware, adware and key loggers that are often secretly installed on a user's computer to track and/or report certain information back to an external source without the user's permission or knowledge.
Adware	Select to enable adware detection and quarantine during the antivirus scan.
Riskware	Select to enable riskware detection and quarantine during the antivirus scan.
Advanced heuristics	Select to enable enhanced antivirus heuristics.
Alert when viruses are detected	Select to have FortiClient provide a notification alert when a threat is detected on your personal computer. When *Alert when viruses are detected* under *AntiVirus Options* is not selected, you will not receive the virus alert dialog box when attempting to download a virus in a web browser.
Pause background scanning on battery power	Select to pause background scanning when your personal computer is operating on battery power.
Enable FortiGuard Analytics	Select to automatically send suspicious files to the FortiGuard Network for analysis.

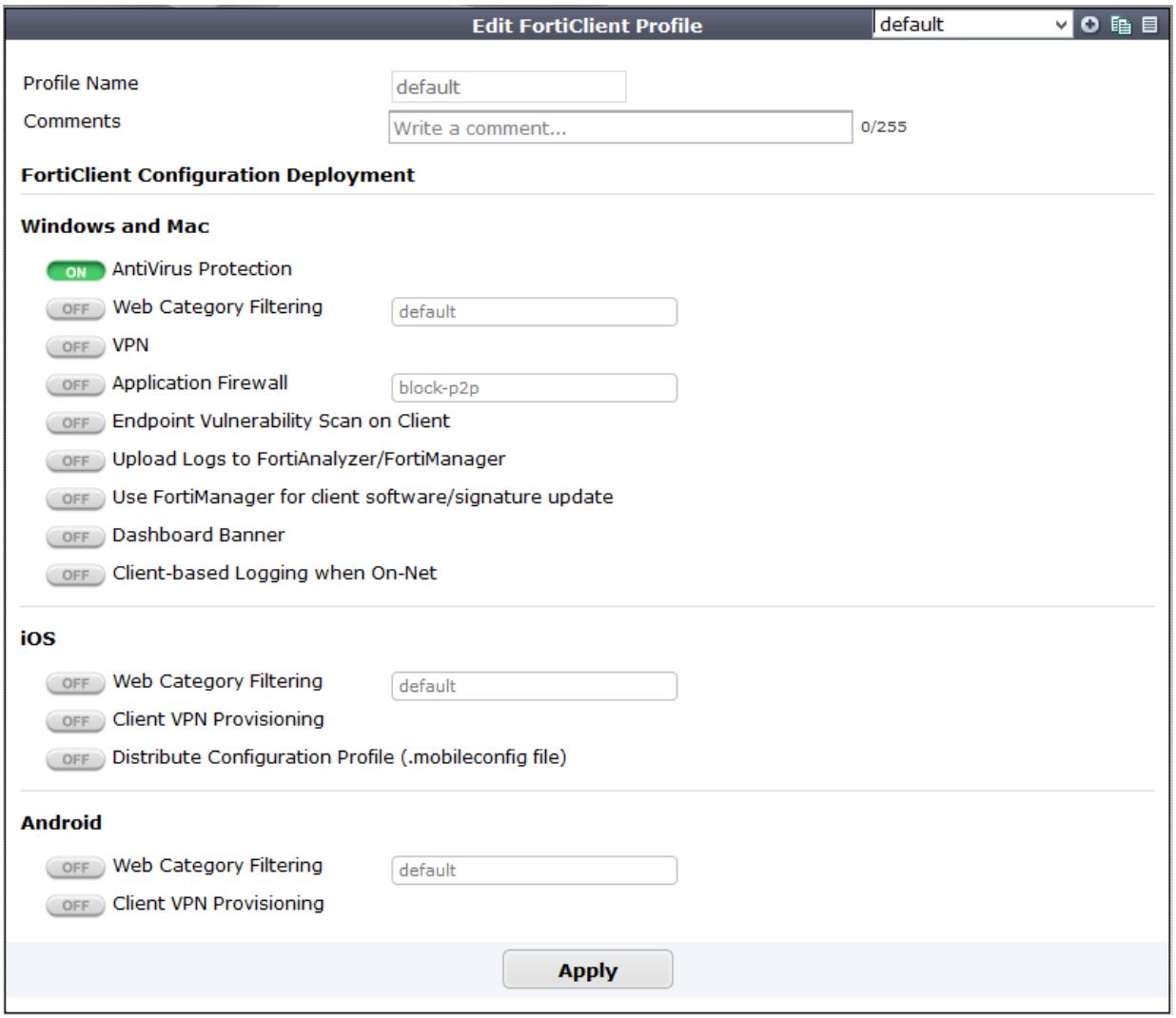
When registered to FortiGate, you can select to enable or disable FortiClient Antivirus Protection in the FortiClient Profile.

Endpoint control

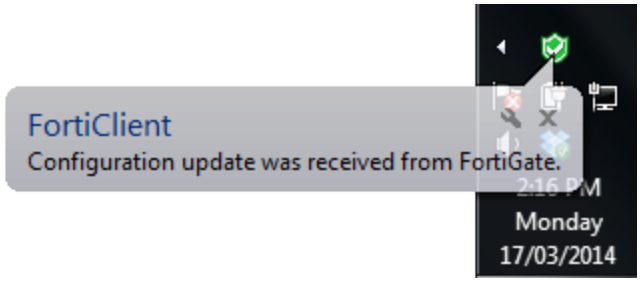
When FortiClient is registered to FortiGate for endpoint control, FortiClient receives configuration and settings via the FortiClient Profile configured on the FortiGate device.

To enable Antivirus Protection in the FortiClient Profile:

1. Log into your FortiGate.
2. In the left tree menu, select *User & Device* > *FortiClient Profiles*.
3. In the right pane, in the *Edit FortiClient Profile* page, in the *FortiClient Configuration Deployment* section, toggle the *AntiVirus Protection* button to *ON*.



4. Select *Apply* to save the profile.
   The FortiGate will send the FortiClient Profile configuration update to registered clients.



Web Security/Web Filter

Web Security/Web Filter allows you to block, allow, warn, and monitor web traffic based on URL category or custom URL filters. URL categorization is handled by the FortiGuard Distribution Network (FDN). You can create a custom URL filter exclusion list which overrides the FDN category.

When FortiClient is not registered to FortiGate, you can enable or disable the Web Security feature. You can define what sites are allowed, blocked, or monitored and view violations.

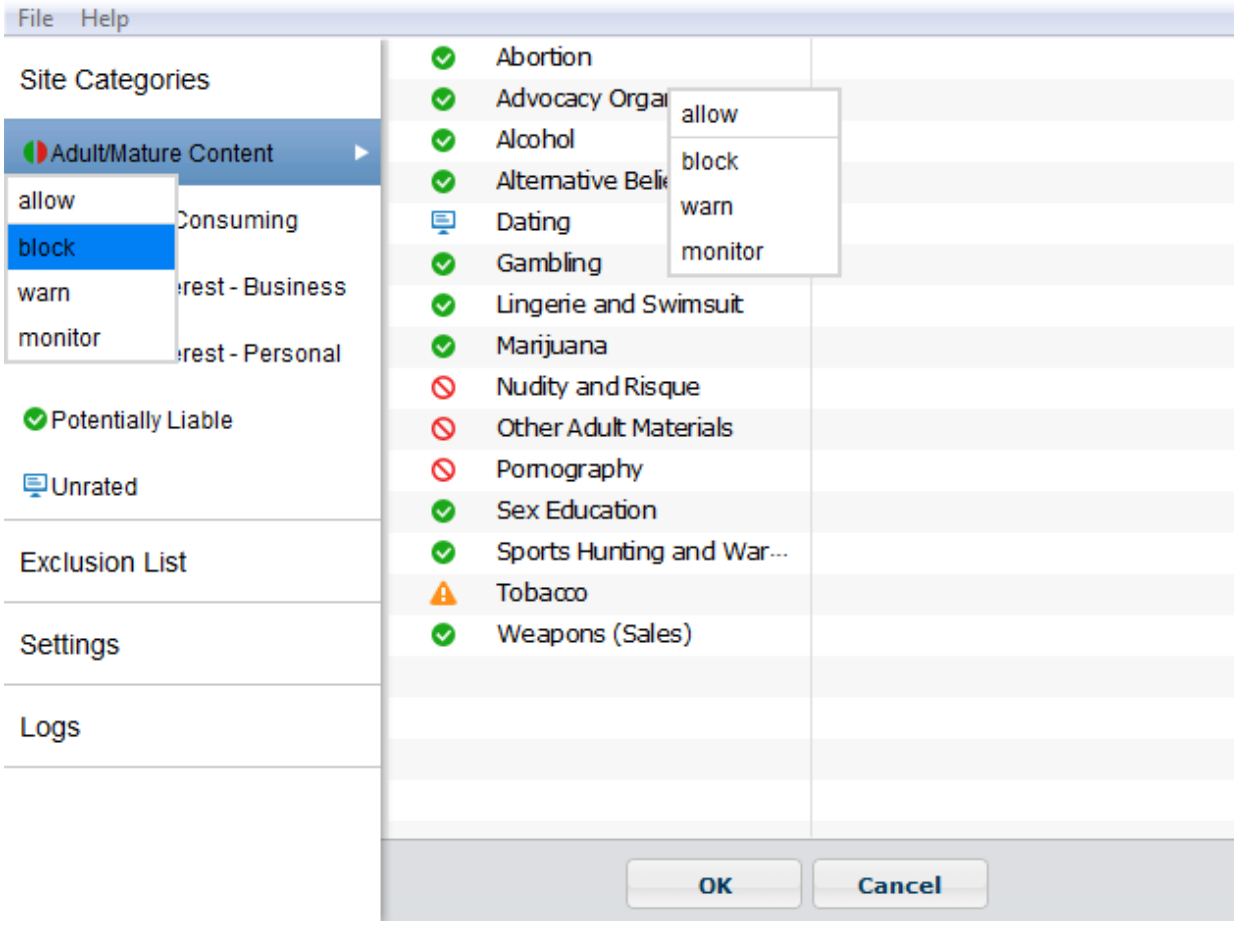
Enable/Disable Web Security

To enable or disable FortiClient Web Security/Web Filtering, toggle the *[Enable/Disable]* link in the FortiClient console. Web Security is enabled by default.

Enable/Disable	Select to enable or disable Web Security.
Violations (In the Last 7 Days)	Select to view Web Security log entries of the violations that have occurred in the last 7 days.
Settings	Select to configure the Web Security profile, exclusion list, settings, and view violations.

Web Security profile

You can configure a Web Security profile to allow, block, warn, or monitor web traffic based on website category and sub-category. Select the settings icon and select the site category. Left-click the action icon and select the action in the menu for each category or sub-category.



Allow	Set the category or sub-category to *Allow* to allow access.
Block	Set the category or sub-category to *Block* to block access. The user will receive a Web Page Blocked message in the web browser.

Warn	Set the category or sub-category to *Warn* to block access. The user will receive a Web Page Blocked message in the web browser. The user can select to proceed or go back to the previous web page.
Monitor	Set the category or sub-category to *Monitor* to allow access. The site will be logged.

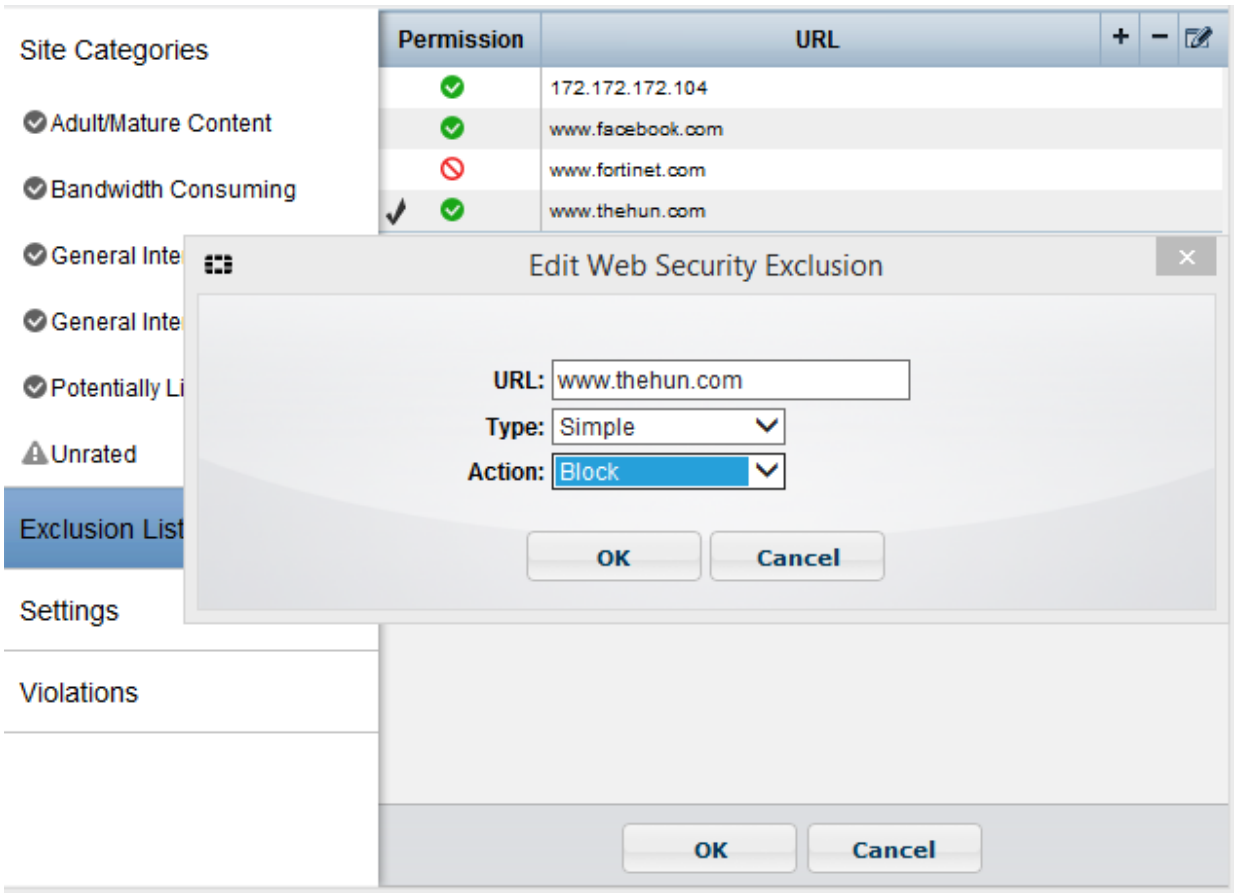
You can select to enable or disable *Site Categories* in the *Web Security* settings page. When site categories are disabled, FortiClient is protected by the exclusion list.

Web Security exclusion list

Select the settings icon and select Exclusion List from the menu. You can add websites to the exclusion list and set the permission to allow, block, monitor, or exempt. Use the add icon to add URLs to the exclusion list. If the website is part of a blocked category, an allow permission in the *Exclusion List* would allow the user to access the specific URL.

For more information on URL formats, type, and action, see the *FortiOS Handbook* available in the Fortinet Document Library.

The following dialog box shows an example Web Security exclusion list.

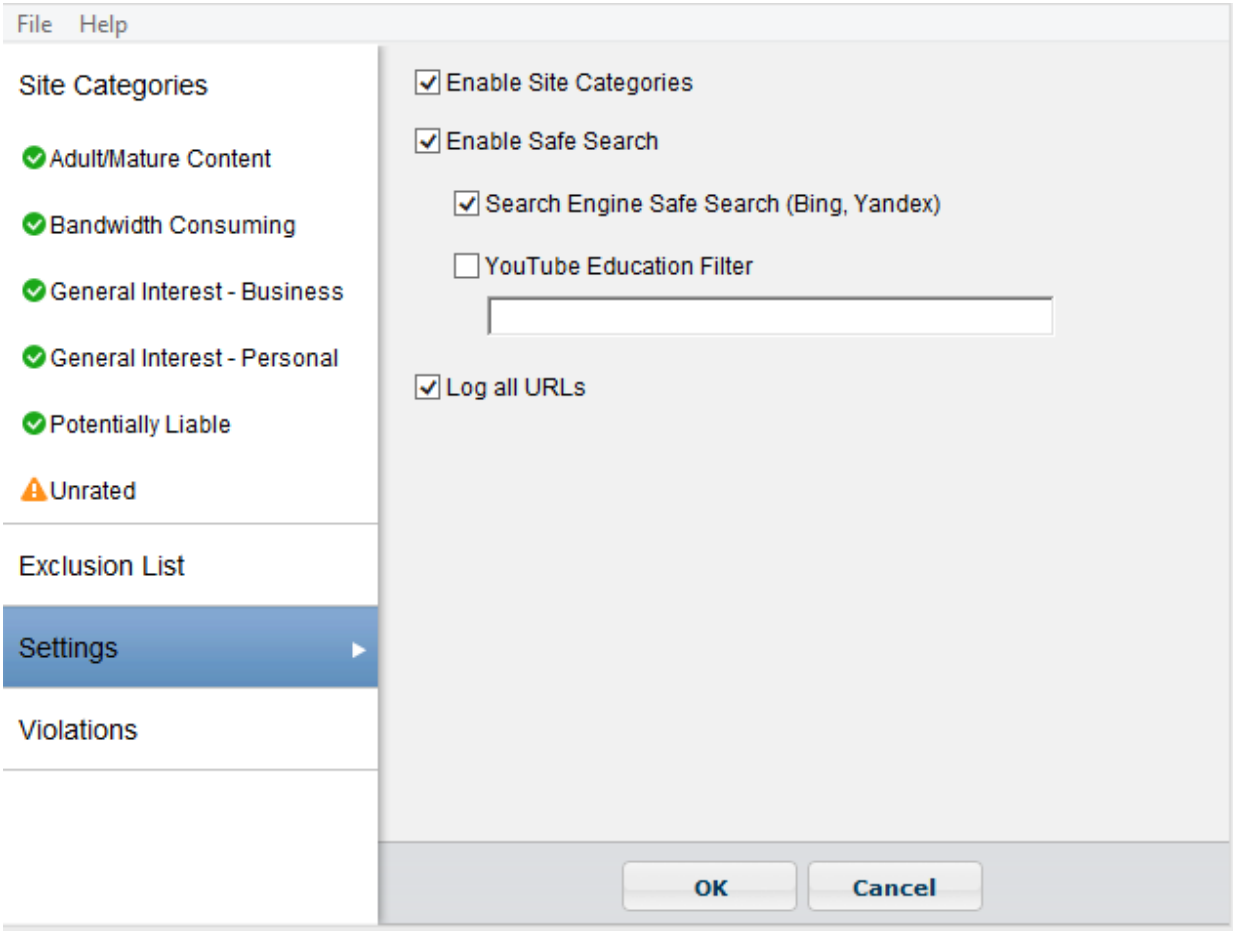


Configure the following settings:

Profile	Select to allow, block, warn or monitor traffic by category or sub-category.
Exclusion List	Select to exclude URLs that are explicitly blocked or allowed. Use the add icon to add URLs and the delete icon to delete URLs from the list. Select a URL and select the edit icon to edit the selection.
URL	Enter a URL or IP address.
Type	Select one of the following pattern types from the drop-down list: • Simple • Wildcard • Regular Expression
Actions	Select one of the following actions from the drop-down list: • Block: Block access to the web site regardless of the URL category or sub-category action. • Allow: Allow access to the web site regardless of the URL category or sub-category action. • Monitor: Allow access to the web site regardless of the URL category or sub-category action. A log message will be generated each time a matching traffic session is established.

Web Security settings

To configure Web Security settings, select the settings icon and select *Settings* from the menu.



Configure the following settings:

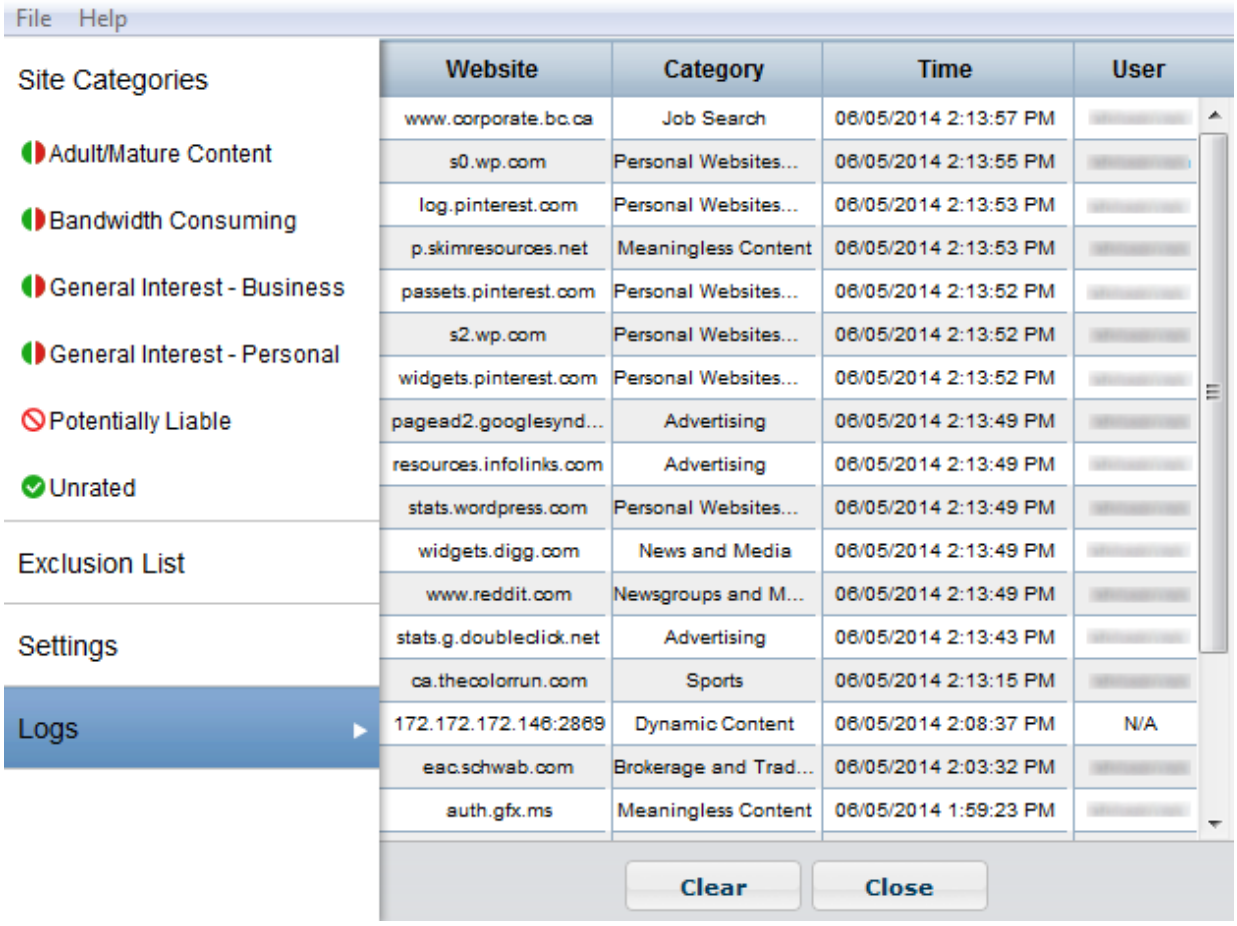
Enable Site Categories	Select to enable Site Categories. When site categories are disabled, FortiClient is protected by the exclusion list.
Enable Safe Search	Select to enable Safe Search.
Search Engine Safe Search	Select to enable search engine Safe Search for Bing and Yandex.
YouTube Education Filter	Select to enable the YouTube educational filter and enter your filter code. The filter blocks non-educational content as per your YouTube filter code.
Log all URLs	Select to log all URLs.

See http://support.google.com/youtube/bin/answer.py?hl=en&answer=2592715 for more information on YouTube for schools and the education filter.

View violations

To view Web Security violations, select the settings icon and select *Violations* from the menu.

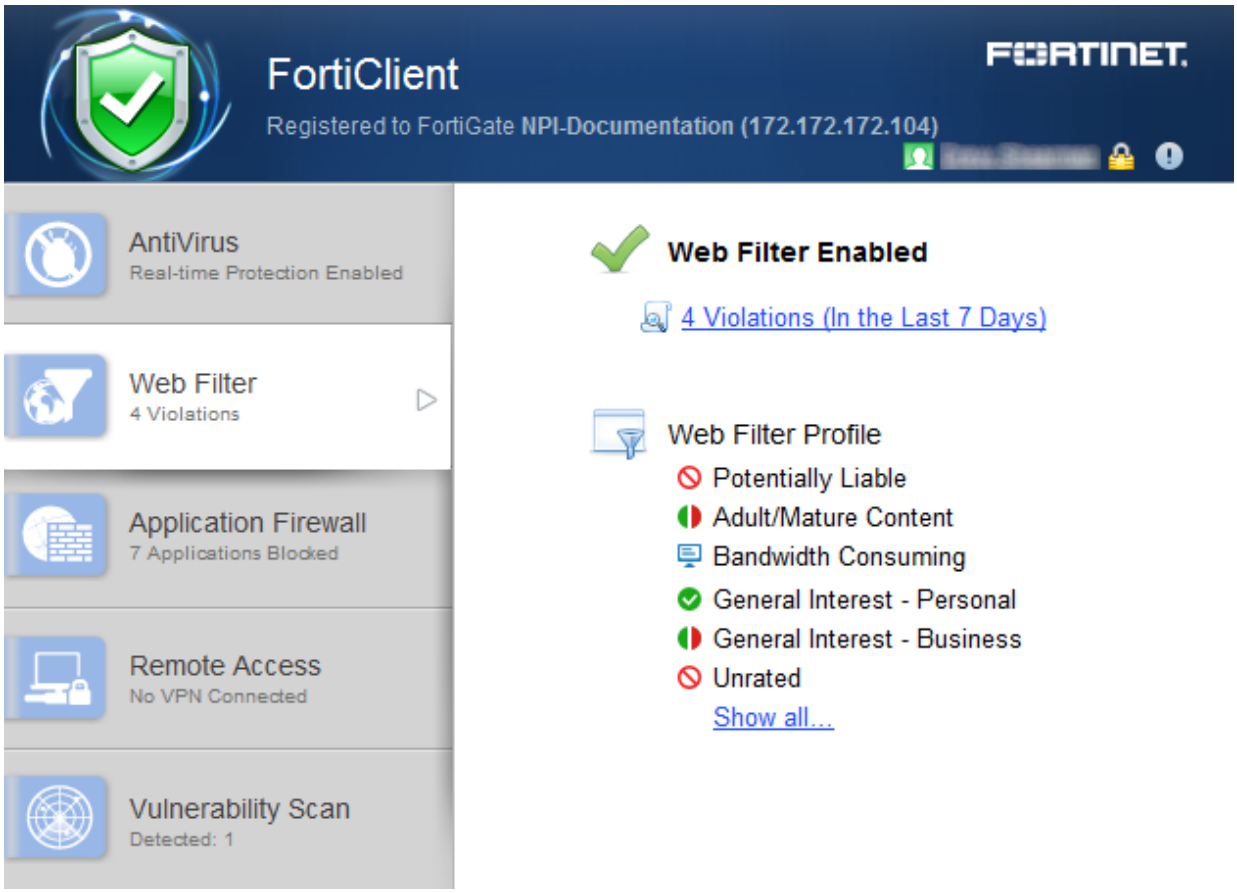
Web Security logs



Website	The website name or IP address.
Category	The website sub-category.
Time	The date and time that the website was accessed.
User	The name of the user generating the traffic. Hover the mouse cursor over the column to view the complete entry in the pop-up bubble message.

Web Filter

When FortiClient is registered to a FortiGate, the *Web Security* module will reflect *Web Filter.*



You can disable *Web Category Filtering* in FortiClient from the FortiGate FortiClient profile. You can also select to enable or disable Web Filtering when the FortiClient device is On-Net. When *FortiGuard Categories* is disabled, FortiClient will be protected by the *Exclusion List* configured in the URL in the FortiClient profile.

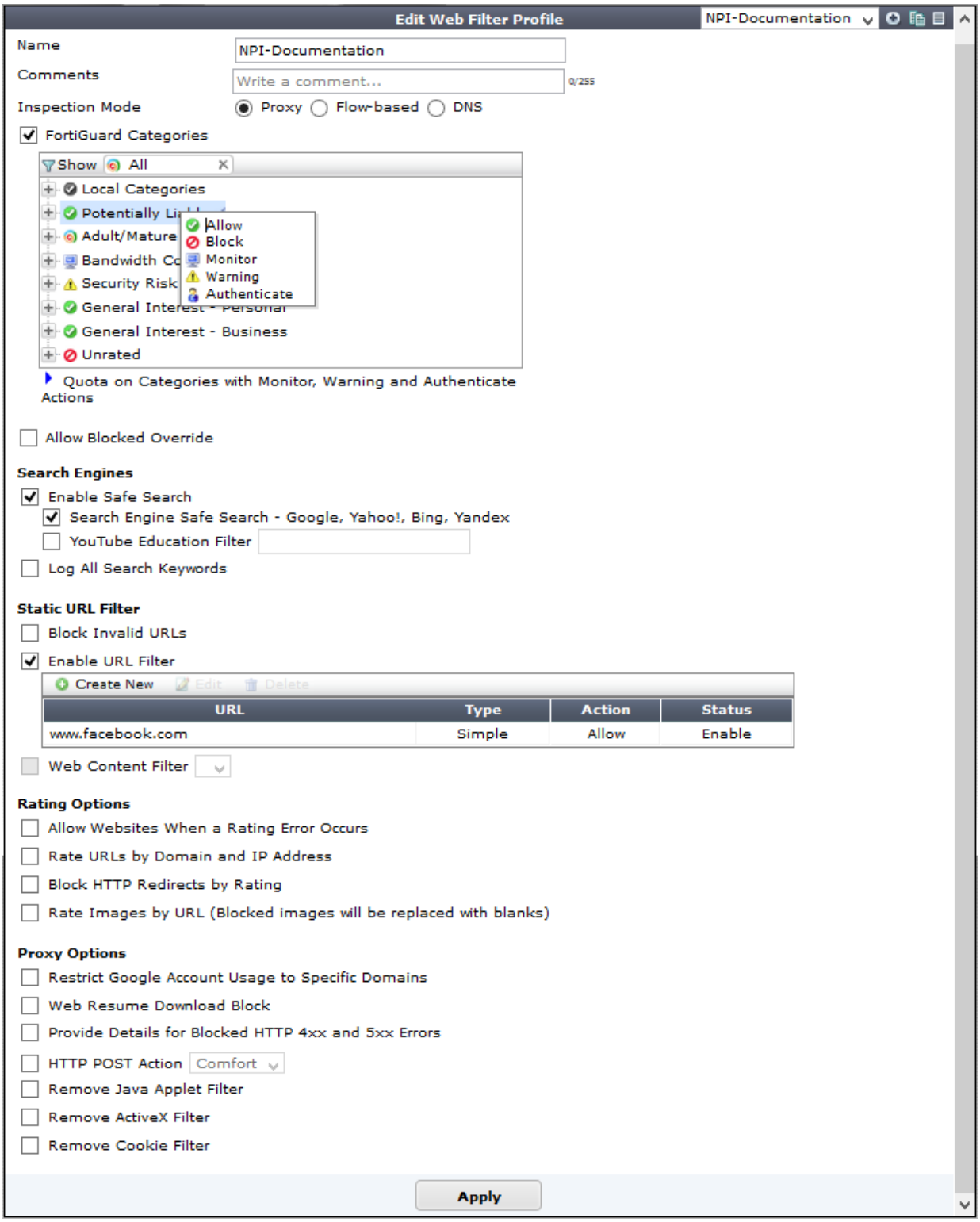
The FortiClient Endpoint Control feature enables the site administrator to distribute a Web Filtering profile from a FortiGate device. The overall process is as follows:

- Create a Web Filter profile on the FortiGate
- Add the Web Filter profile to the FortiClient Profile on the FortiGate

Step 1: Create a Web Filter Profile on the FortiGate

Use the following steps to create a custom Web Filter profile on the FortiGate GUI:

1. Go to *Security Profiles* > *Web Filter*.
2. To create a new profile, click the create new icon in the toolbar. The *New Web Filter Profile* page opens.



3. Configure the following settings:

Name	Enter a name for the Web Filter profile.

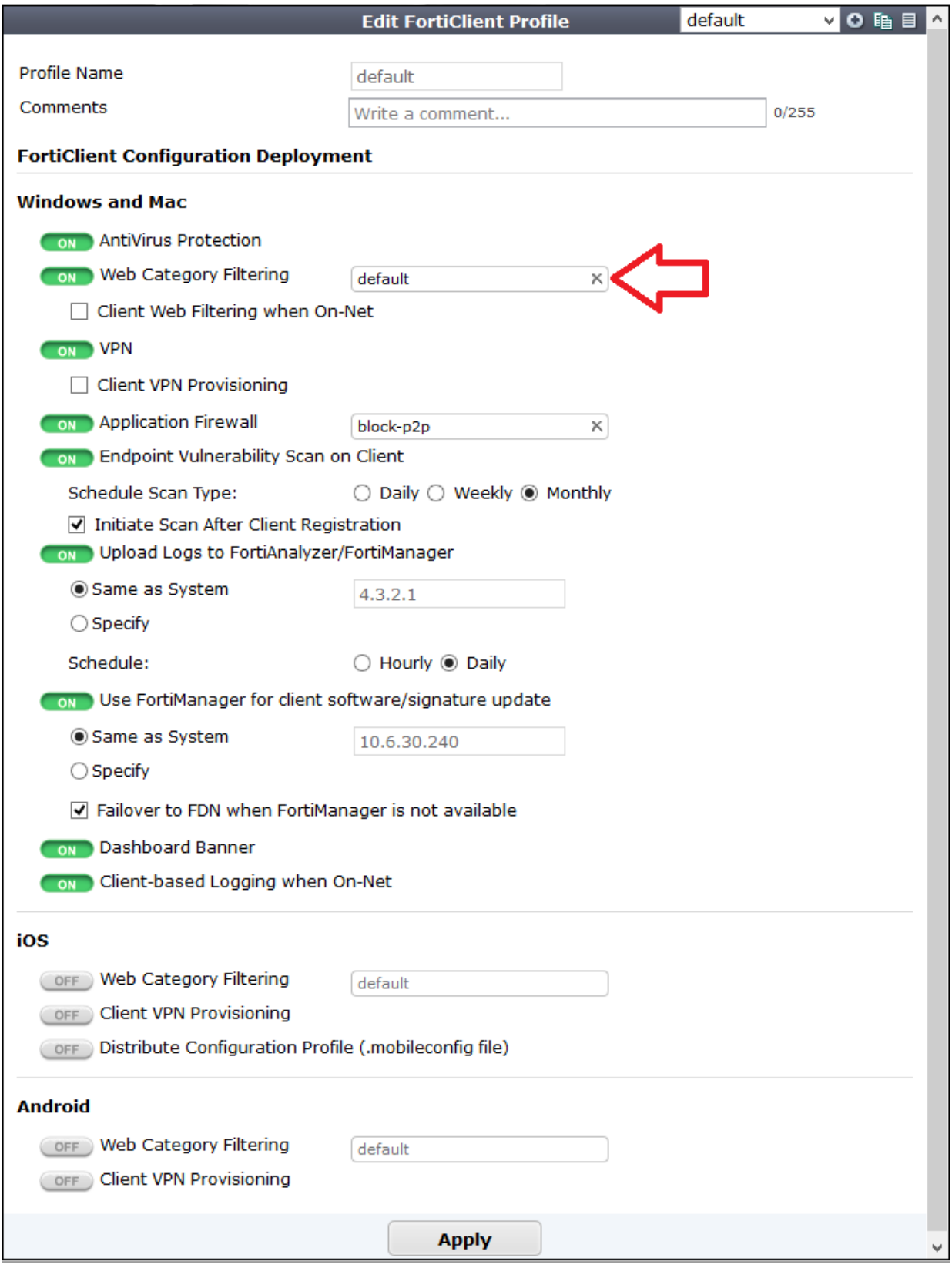
Comments	Enter a description in the comments field. (optional)
Inspection Mode	This setting is not applicable to FortiClient.
FortiGuard Categories	Select category and sub-category actions. • In FortiClient 5.2.6, the *Security Risk* category is part of the AntiVirus module. The Local Categories category is not applicable to FortiClient. The *Authenticate* and *Disable* actions are not applicable to FortiClient. • When *FortiGuard Categories* is disabled, FortiClient will be protected by the *Exclusion List* configured in the URL in the FortiClient profile.
Quota on Categories ...	This setting is not applicable to FortiClient.
Allow Blocked Override	This setting is not applicable to FortiClient.
Search Engines	
Enable Safe Search	Select to enable Safe Search.
Search Engine Safe Search	Select to enable search engine Safe Search for Bing and Yandex. Search engine safe search for Google and Yahoo! is currently not supported.
YouTube Education Filter	Select to enable the YouTube educational filter and enter your filter code. The filter blocks non-educational content as per your YouTube filter code.
Log All Search Keywords	This setting is not applicable to FortiClient.
Static URL Filter	
Block Invalid URLs	This setting is not applicable to FortiClient.
Enable URL Filter	Select to enable URL filter. Select *Create New* to add a URL to the list. For *Type*, select one of *Simple*, *Reg. Expression*, or *Wildcard*. For *Action*, select one of *Exempt*, *Block*, *Allow*, or *Monitor*. For *Status*, select either *Enable* or *Disable*. FortiClient does not support the Exempt action. Any URLs in the URL filter with an exempt action will be added to the FortiClient Exclusion List with an allow action.
Web Content Filter	This setting is not applicable to FortiClient.
Rating Options	These settings are not applicable to FortiClient.
Proxy Options	These settings are not applicable to FortiClient.

4. Select *OK* to save the profile.

If the FortiGate device is not licensed, you will receive an dialog box advising that traffic may be blocked if this option is enabled.

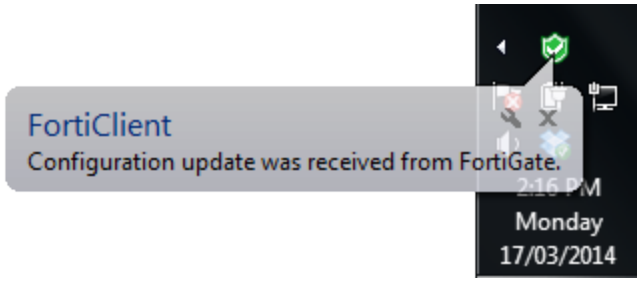
Step 2: Add the Web Filter profile to the FortiClient Profile

1. Go to *User & Device* > *FortiClient Profiles*.
2. Select the FortiClient Profile and select *Edit* in the toolbar. The *Edit FortiClient Profile* page is displayed.



3. Toggle the *Web Category Filtering* button to *ON* and select the Web Filter profile from the drop-down list.

4. Optionally, select to enable *Client Web Filtering when On-Net*.
5. Select *Apply* to save the profile.
   The FortiGate will send the FortiClient Profile configuration update to registered clients.



The Web Filtering module is now available in FortiClient.

The following dialog box illustrates web filter profile settings received by the FortiGate endpoint control profile.

Application Firewall

FortiClient can recognize the traffic generated by a large number of applications. You can create rules to block or allow this traffic per category, or application.

In FortiClient v5.2 this feature is disabled by default and the tab is hidden for standalone clients. For uses who are registered to a FortiGate using endpoint control, the FortiGate administer may choose to enable this feature.

For more information on configuring application control security profiles, see the *FortiOS Handbook - The Complete Guide to FortiOS* available in the Fortinet Document Library.

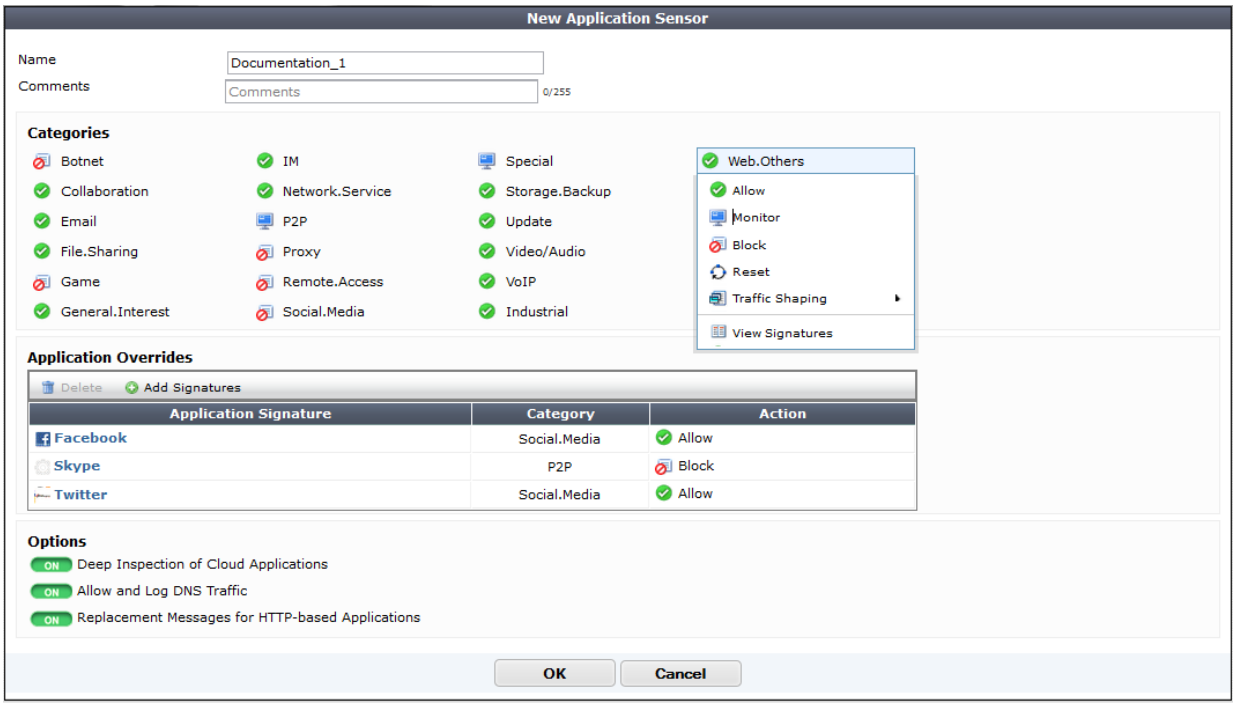
In FortiClient v5.2, the application firewall feature is enabled in the FortiClient Profile. The profile includes application firewall configuration.

The FortiClient Endpoint Control feature enables the site administrator to distribute an Application Control sensor from a FortiGate device. The process is as follows:

- Create an Application Sensor and Application Filter on the FortiGate
- Add the Application Sensor to the FortiClient Profile on the FortiGate

Step 1: Create a custom Application Control Sensor

1. Login to your FortiGate.
2. In the left tree menu, select *Security Profiles* > *Application Control*.
3. To create a new sensor, click the *Create New* icon in the toolbar. The *New Application Sensor* page is displayed.



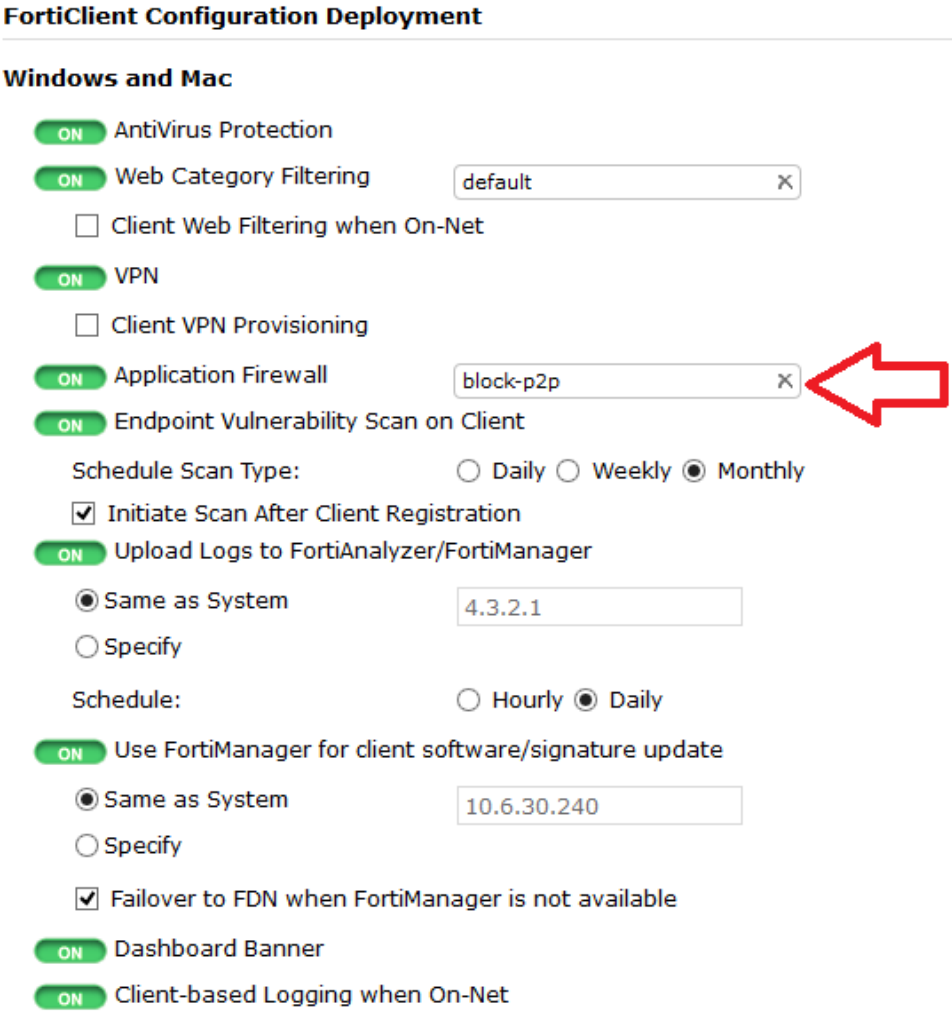
4. Configure the following options:

Name	Enter a unique name for the application sensor.
Comments	Enter an option comment for the application sensor.
Categories	Select categories to allow or block.
Allow	The application category or application signature will be allowed in FortiClient Application Firewall.
Block	The application category or application signature will be blocked in FortiClient Application Firewall.
Monitor	The application category or application signature will be allowed in FortiClient Application Firewall. FortiClient will allow application traffic but will not monitor.
Reset	The application category or application signature will be blocked in FortiClient Application Firewall.
Traffic Shaping	The application category or application signature will be allowed in FortiClient Application Firewall. FortiClient will allow application traffic but will not enforce traffic shaping settings.
Application Overrides	Select *Add Signatures* to add application signatures and set the category. An application which belongs to a blocked category can be set to allow.
Options	The options set in the FortiOS application sensor are ignored by FortiClient application firewall.

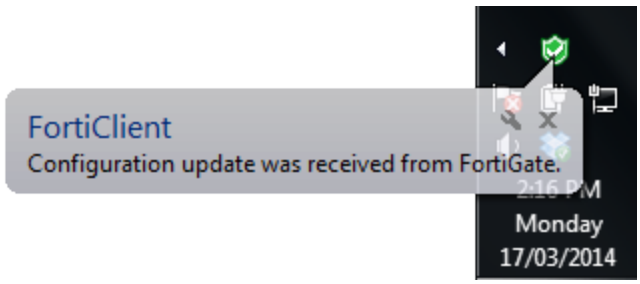
5. Select *OK* to save the sensor.

Step 2: Add the Application Control Sensor to the FortiClient Profile

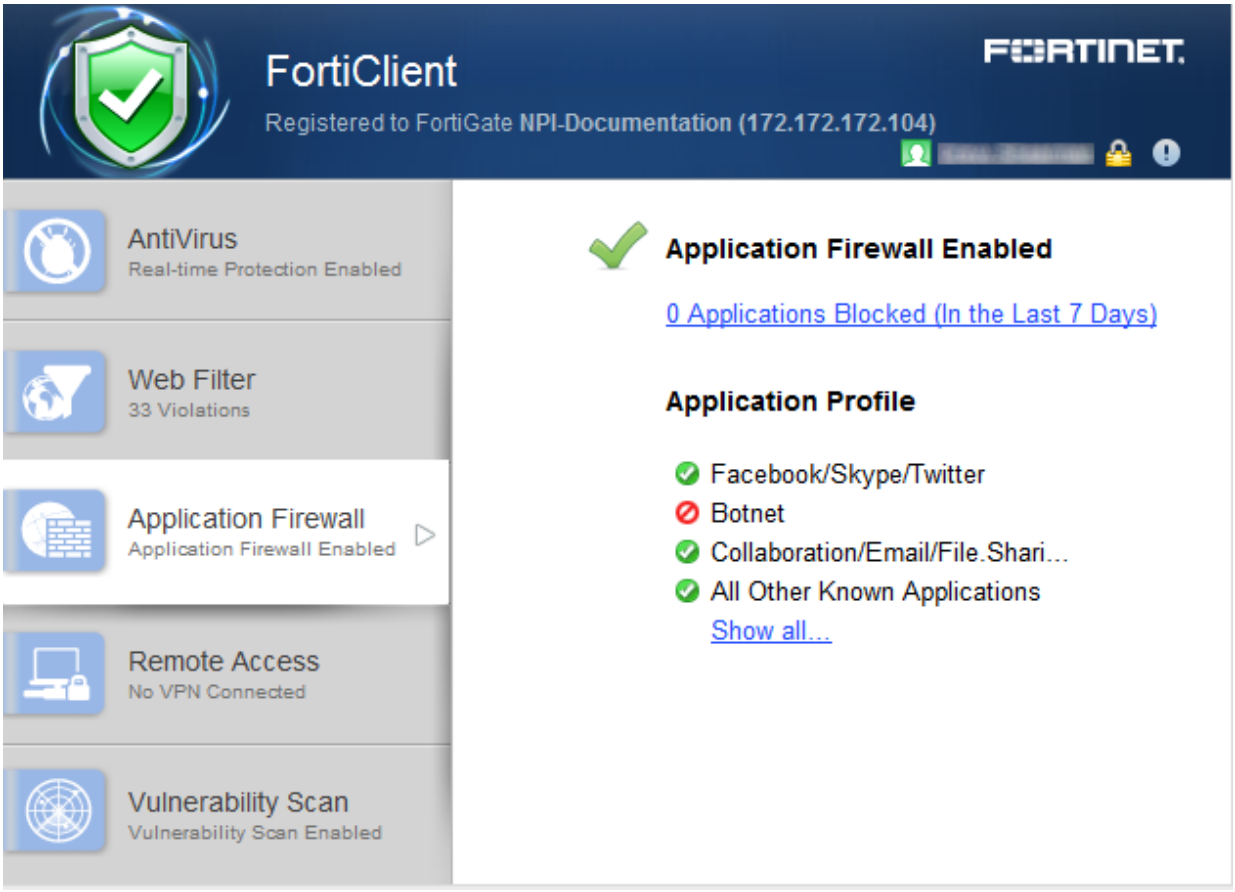
1. In the left tree menu, select *User & Device* > *FortiClient Profiles*.
2. Select the FortiClient Profile and select *Edit* in the toolbar. The *Edit FortiClient Profile* page is displayed.



3. In the right pane, toggle the *Application Firewall* button to *ON*.
4. Select the Application Sensor from the drop-down list.
5. Select *Apply* to save the profile.
   The FortiGate will send the FortiClient Profile configuration update to registered clients.

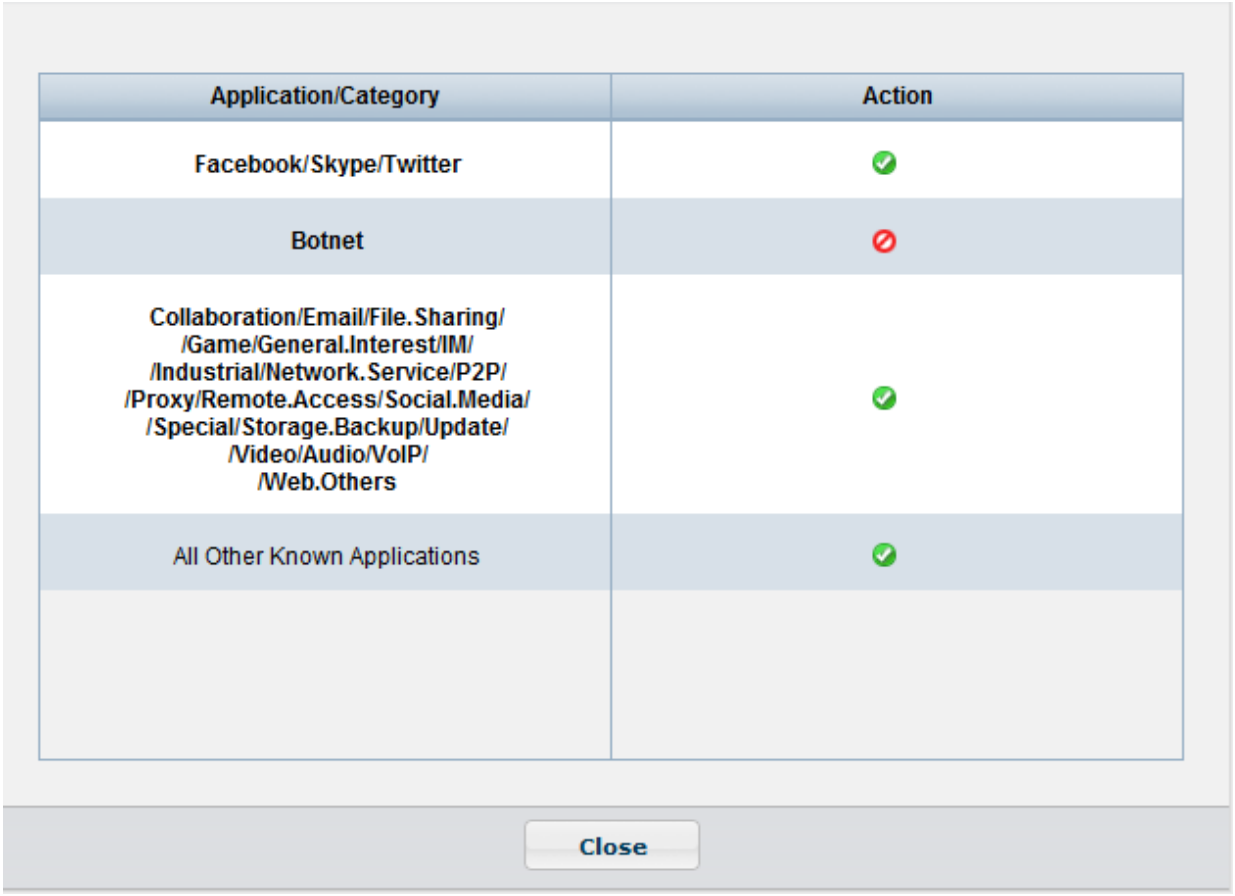


The Application Control module is now available in FortiClient.



View application firewall profile

To view the application firewall profile, select *Show all*.



View blocked applications

To view blocked applications, select the *Applications Blocked* link in the FortiClient console. This page lists all applications blocked in the past seven days, including the count and time of last occurrence.

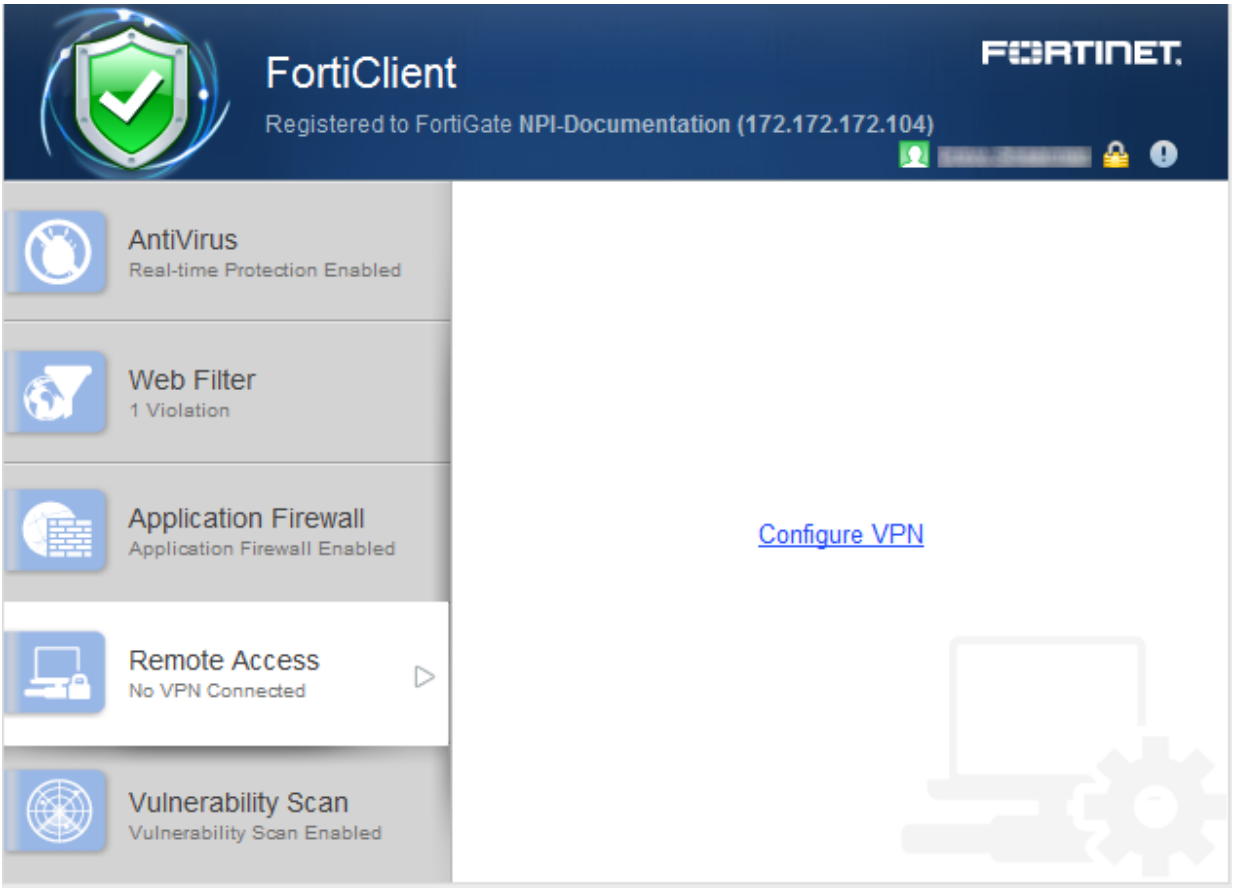
IPsec VPN and SSL VPN

FortiClient supports both IPsec and SSL VPN connections to your network for remote access. You can provision client VPN connections in the FortiClient Profile or configure new connections in the FortiClient console.

This section describes how to configure remote access.

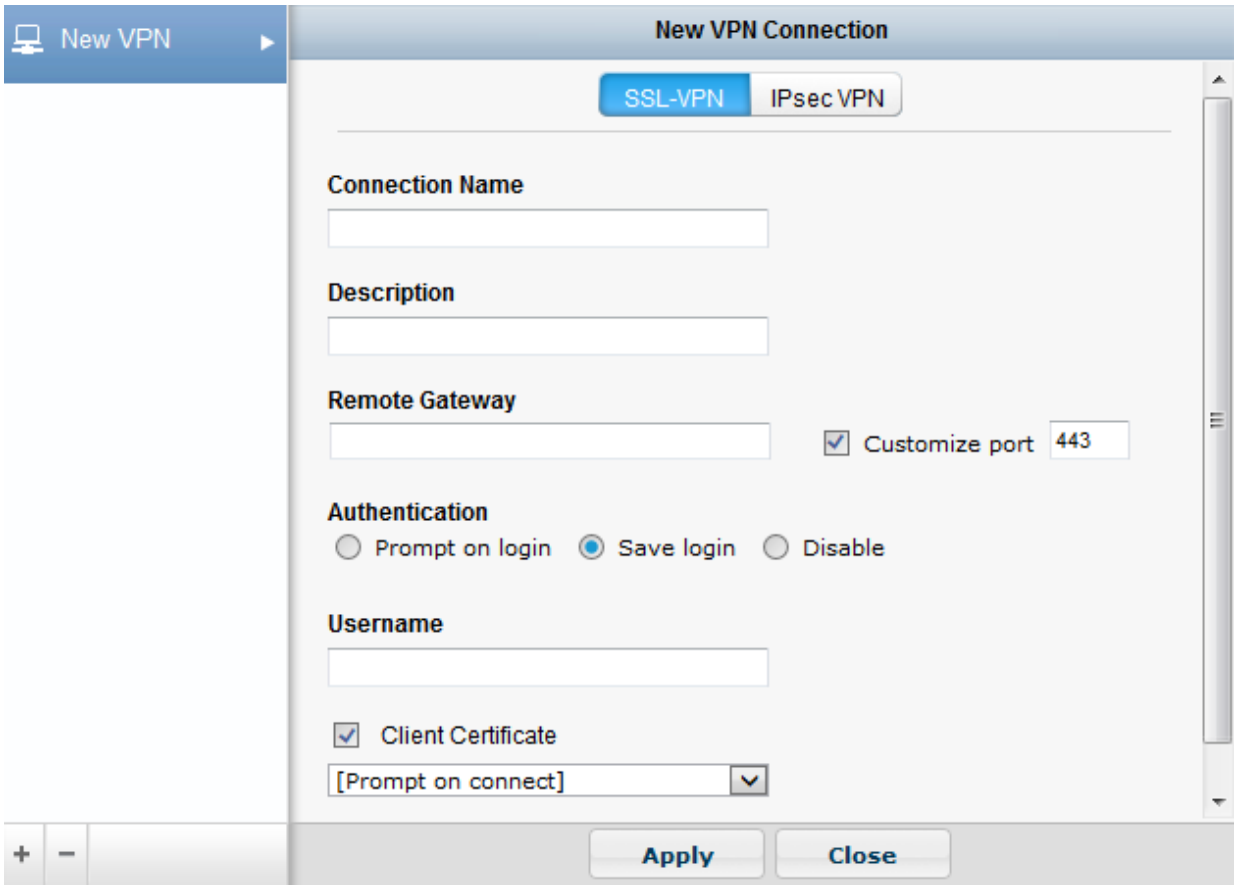
Add a new connection

Select *Configure VPN* in the FortiClient console to add a new VPN configuration.



Create a new SSL VPN connection

To create a new SSL VPN connection, select *Configure VPN* or use the drop-down menu in the FortiClient console. In this menu you can configure options outlined in the following figure and table.



Configure the following settings:

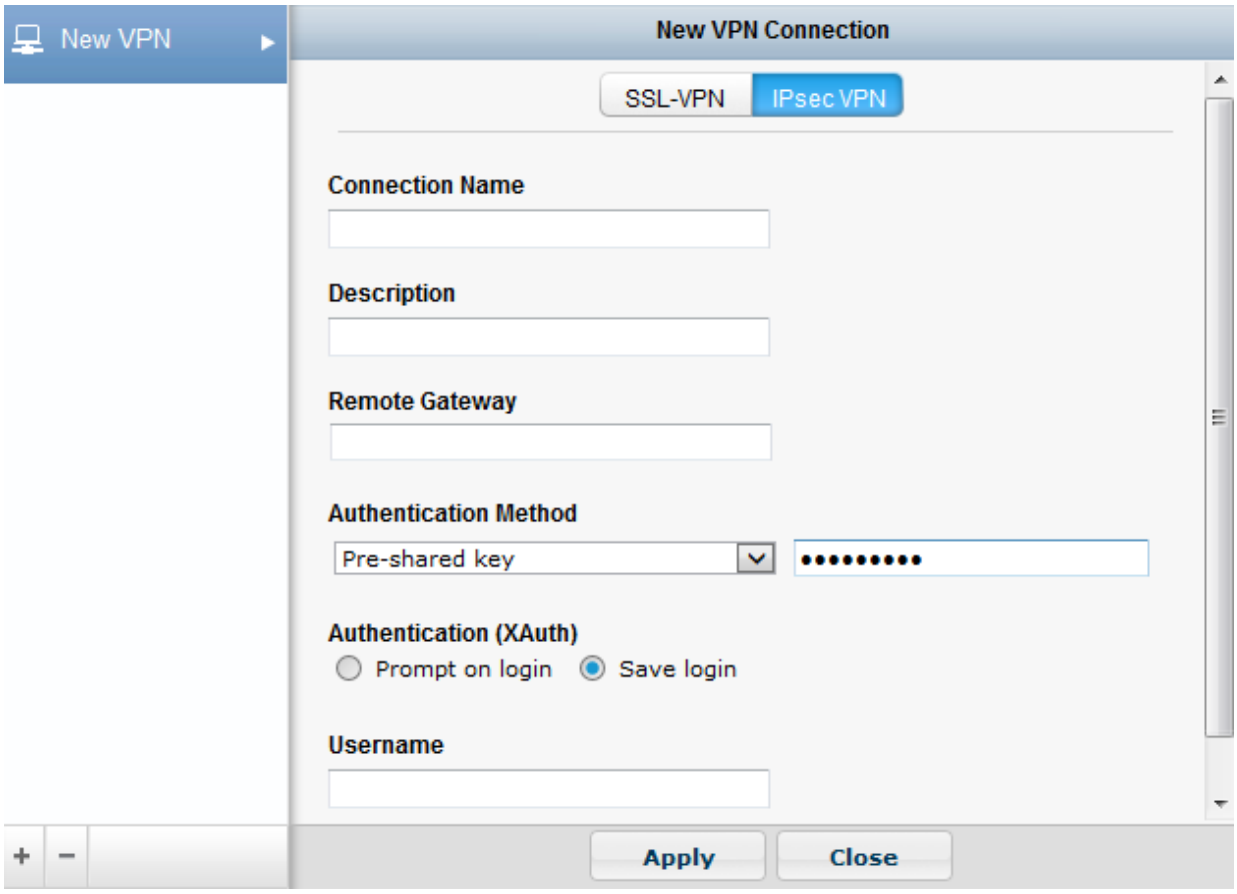
New VPN	Select SSL VPN.
Connection Name	Enter a name for the connection.
Description	Enter a description for the connection. (optional)
Remote Gateway	Enter the IP address/hostname of the remote gateway. Multiple remote gateways can be configured by separating each entry with a semicolon. If one gateway is not available, the VPN will connect to the next configured gateway.
Customize port	Select to change the port. The default port is 443.
Authentication	Select to prompt on login, or save login. The option to disable is available when *Client Certificate* is enabled.
Username	If you selected to save login, enter the username in the dialog box.
Client Certificate	Select to enable client certificates.

Certificate	Select the certificate option in the drop-down list.
Do not Warn Invalid Server Certificate	Select if you do not want to warned if the server presents an invalid certificate.
Add	Select the add icon to add a new connection.
Delete	Select a connection and then select the delete icon to delete a connection.

Select *Apply* to save the VPN connection and select *Close* to return to the Remote Access screen.

Create a new IPsec VPN connection

To create a new IPsec VPN connection, select *Configure VPN* or use the drop-down menu in the FortiClient console. In this menu you can configure options outlined in the following figure and table.



Configure the following settings:

Connection Name	Enter a name for the connection.
Type	Select IPsec VPN.

Description	Enter a description for the connection. (optional)
Remote Gateway	Enter the IP address/hostname of the remote gateway. Multiple remote gateways can be configured by separating each entry with a semicolon. If one gateway is not available, the VPN will connect to the next configured gateway.
Authentication Method	Select either *X.509 Certificate* or *Pre-shared Key* in the drop-down menu.
X.509 Certificate, Pre-shared Key	Select *X.509 Certificate* in the drop-down menu, or enter the pre-shared key in the dialog box. See Certificate management on page 131 for information on configuring certificate options.
Authentication (XAuth)	Select to prompt on login, save login, or disable.
Username	If you selected save login, enter the username in the dialog box.
Advanced Settings	Configure VPN settings, Phase 1, and Phase 2 settings.
VPN Settings	
Mode	Select one of the following: • Main: In Main mode, the phase 1 parameters are exchanged in multiple rounds with encrypted authentication information. • Aggressive: In Aggressive mode, the phase 1 parameters are exchanged in a single message with authentication information that is not encrypted. Although Main mode is more secure, you must select Aggressive mode if there is more than one dialup phase 1 configuration for the interface IP address, and the remote VPN peer or client is authenticated using an identifier (local ID).
Options	Select one of the following: • Mode Config: IKE Mode Config can configure host IP address, Domain, DNS and WINS addresses. • Manually Set: Manual key configuration. If one of the VPN devices is manually keyed, the other VPN device must also be manually keyed with the identical authentication and encryption keys. Enter the DNS server IP, assign IP address, and subnet values. Select the check box to enable split tunneling. • DHCP over IPsec: DHCP over IPsec can assign an IP address, Domain, DNS and WINS addresses. Select the check box to enable split tunneling.

Phase 1		Select the encryption and authentication algorithms used to generate keys for protecting negotiations and add encryption and authentication algorithms as required. You need to select a minimum of one and a maximum of two combinations. The remote peer or client must be configured to use at least one of the proposals that you define.
	IKE Proposal	Select symmetric-key algorithms (encryption) and message digests (authentication) from the drop-down lists.
	DH Group	Select one or more Diffie-Hellman groups from DH group 1, 2, 5 and 14. At least one of the DH Group settings on the remote peer or client must match one the selections on the FortiGate unit. Failure to match one or more DH groups will result in failed negotiations.
	Key Life	Enter the time (in seconds) that must pass before the IKE encryption key expires. When the key expires, a new key is generated without interrupting service. The key life can be from 120 to 172,800 seconds.
	Local ID	Enter the Local ID (optional). This Local ID value must match the peer ID value given for the remote VPN peer's Peer Options.
	Dead Peer Detection	Select this check box to reestablish VPN tunnels on idle connections and clean up dead IKE peers if required.
	NAT Traversal	Select the check box if a NAT device exists between the client and the local FortiGate unit. The client and the local FortiGate unit must have the same NAT traversal setting (both selected or both cleared) to connect reliably.
Phase 2		Select the encryption and authentication algorithms that will be proposed to the remote VPN peer. You can specify up to two proposals. To establish a VPN connection, at least one of the proposals that you specify must match configuration on the remote peer.
	IKE Proposal	Select symmetric-key algorithms (encryption) and message digests (authentication) from the drop-down lists.
	Key Life	The Key Life setting sets a limit on the length of time that a phase 2 key can be used. The default units are seconds. Alternatively, you can set a limit on the number of kilobytes (KB) of processed data, or both. If you select both, the key expires when either the time has passed or the number of KB have been processed. When the phase 2 key expires, a new key is generated without interrupting service.
	Enable Replay Detection	Replay detection enables the unit to check all IPsec packets to see if they have been received before. If any encrypted packets arrive out of order, the unit discards them.

	Enable Perfect Forward Secrecy (PFS)	Select the check box to enable Perfect forward secrecy (PFS). PFS forces a new Diffie-Hellman exchange when the tunnel starts and whenever the phase 2 key life expires, causing a new key to be generated each time.
	DH Group	Select one Diffie-Hellman (DH) group (1, 2, 5 or 14). This must match the DH Group that the remote peer or dialup client uses.
	Auto Keep Alive	Select the check box if you want the tunnel to remain active when no data is being processed.
Add		Select the add icon to add a new connection.
Delete		Select a connection and then select the delete icon to delete a connection.

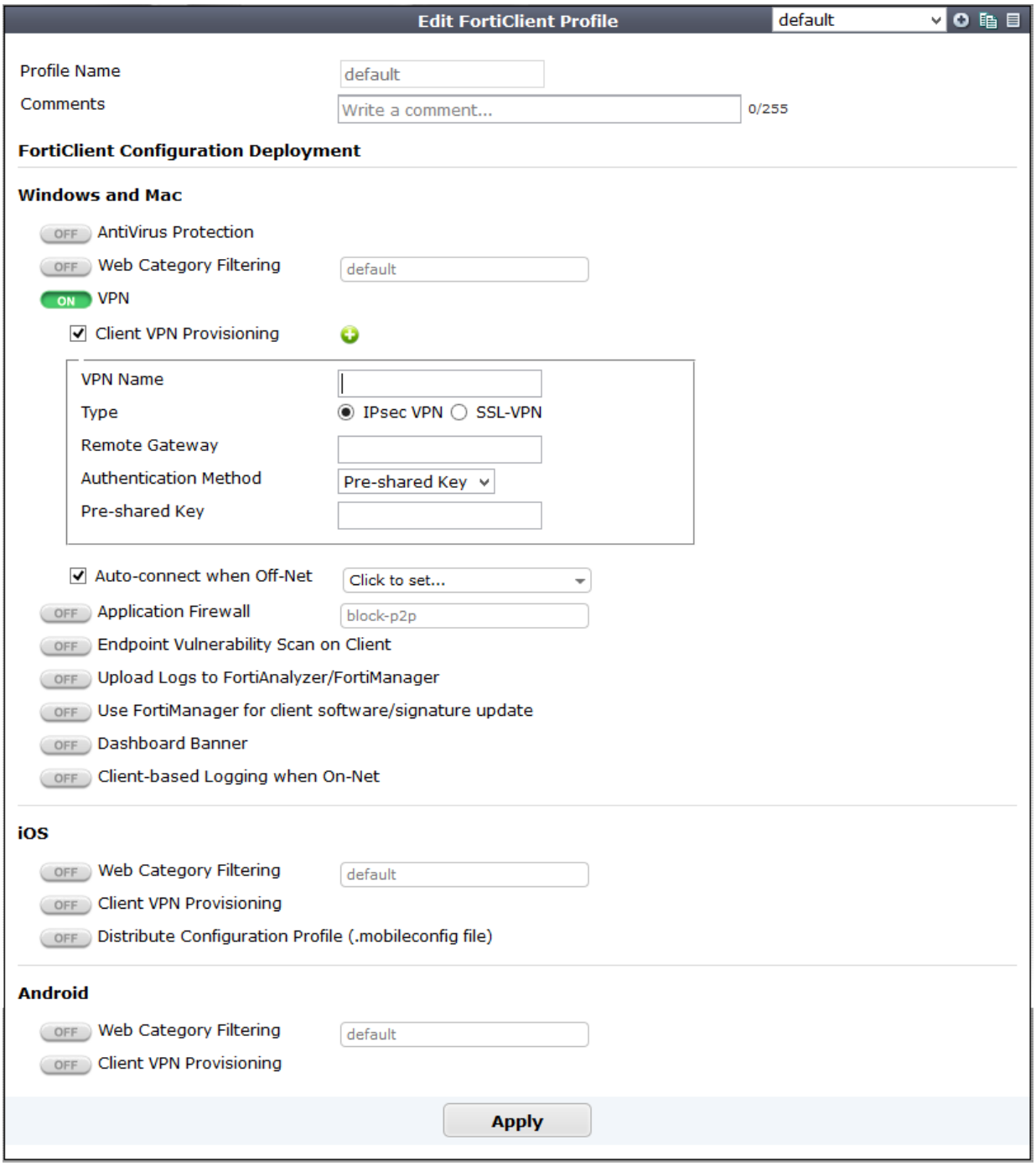
Select *Apply* to save the VPN connection and select *Close* to return to the Remote Access screen.

Provision client VPN connections

You can provision client VPN connections in the FortiClient Profile for registered clients.

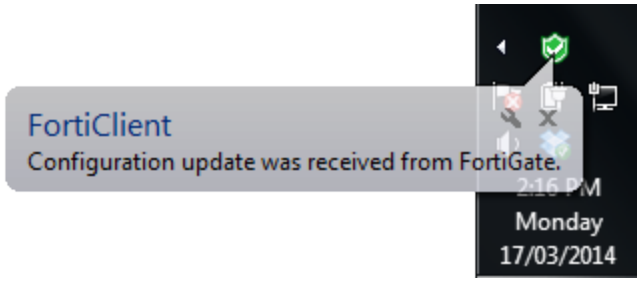
To provision a client VPN in the FortiClient Profile:

1. Login to your FortiGate device.
2. In the left tree menu, select *User & Device* > *FortiClient Profiles*.
3. Select the FortiClient profile and select *Edit* from the toolbar.
4. Edit FortiClient Profile



5. In the *Edit FortiClient Profile* page, in the *FortiClient Configuration Deployment* section, toggle the *VPN* button to *ON*.
6. Select the *Client VPN Provisioning* checkbox.
7. Enter a name for the VPN connection.
8. Select the VPN type. Select either *IPsec VPN* or *SSL-VPN*.
9. Configure the remote gateway and authentication settings for the type of VPN selected.
10. Select the checkbox to auto-connect when off-net and select a VPN connection from the drop-down list.
11. Select *Apply* to save the profile.

The FortiGate will send the FortiClient Profile configuration update to registered clients.

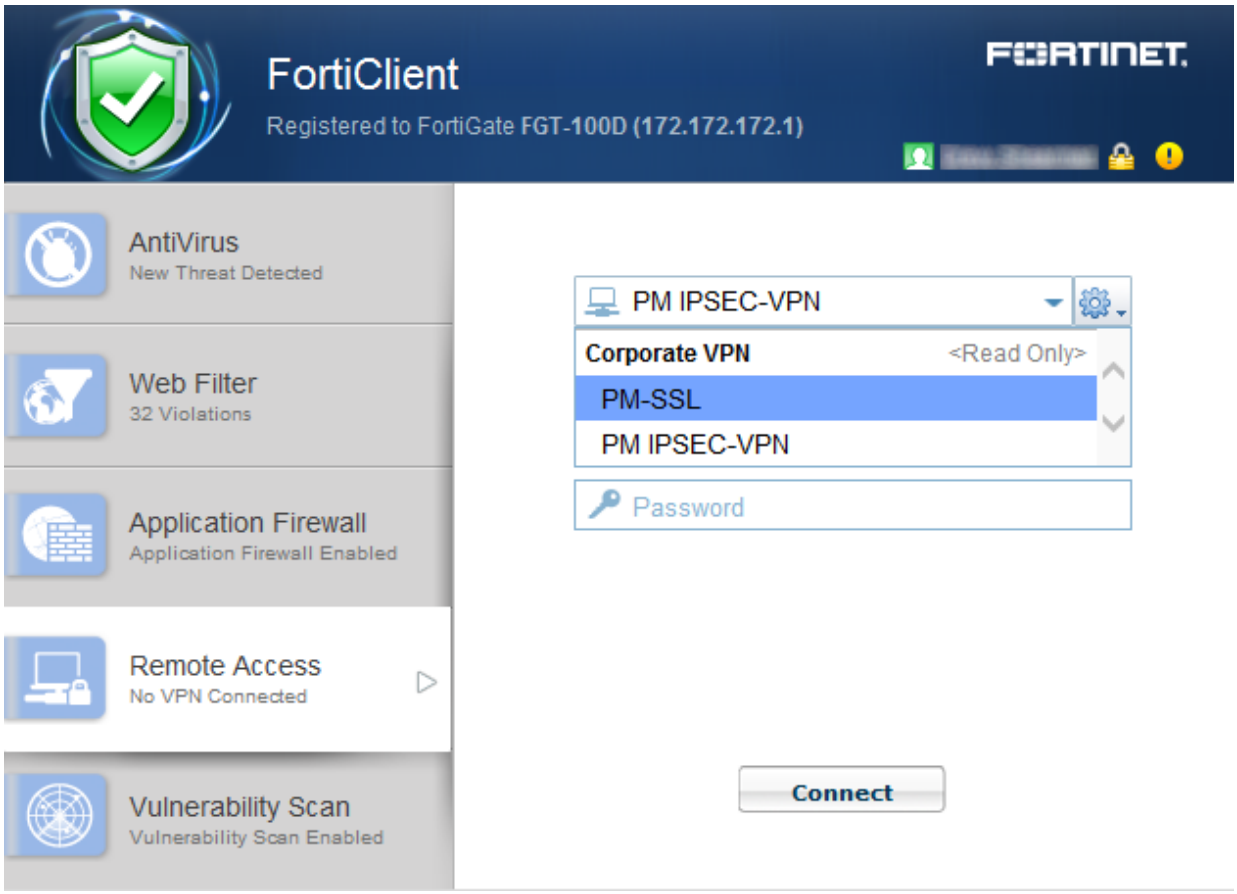


The following dialog box illustrates VPN settings received by the FortiGate FortiClient Profile. When registered to a FortiGate, VPN settings are enabled and configured in the FortiClient Profile.

Alternatively, you can provision a client VPN using the advanced VPN FortiClient Profile options in FortiGate. For more information, see the *FortiClient XML Reference* and the *CLI Reference for FortiOS*.

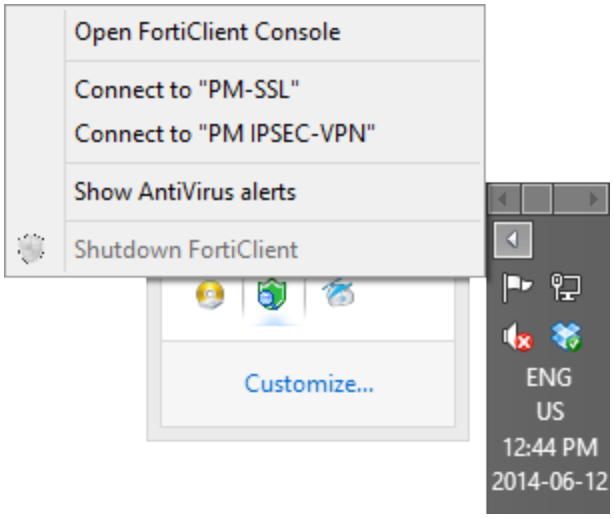
Connect to a VPN

To connect to a VPN, select the VPN connection from the drop-down menu. Enter your username, password, and select the *Connect* button.



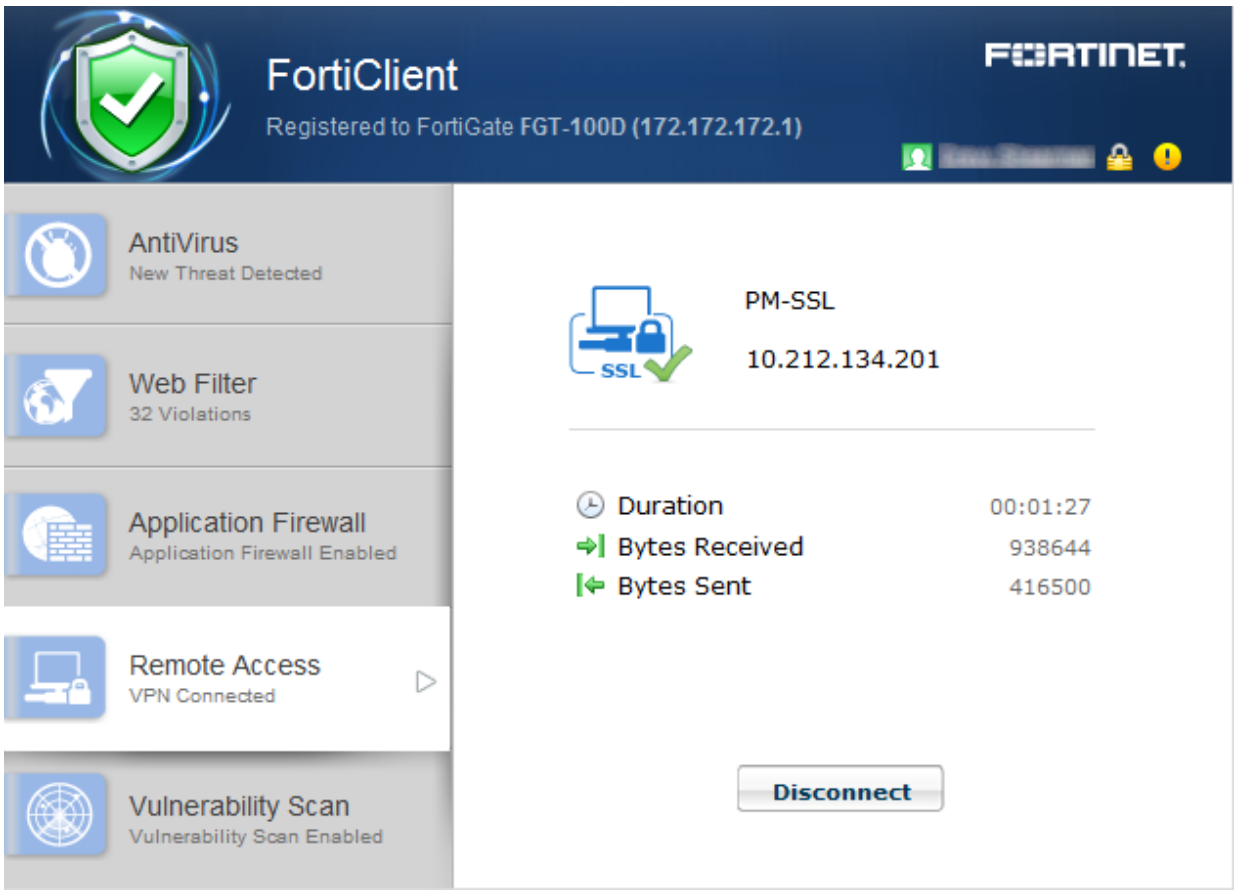
Provisioned VPN connections will be listed under *Corporate VPN*. Locally configured VPN connections will be listed under *Personal VPN*.

Optionally, you can click on the system tray, right-click the FortiClient icon and select the VPN connection you want to connect to.



You can also select to edit an existing VPN connection and delete an existing VPN connection using the drop-down menu.

When connected, the console will display the connection status, duration, and other relevant information. You can now browse your remote network. Select the *Disconnect* button when you are ready to terminate the VPN session.



This page displays the following:

Name of the VPN connection	
Status	The status of the VPN connection.
Duration	The duration of the VPN connection.
Bytes Received	Bytes received through the VPN connection.
Bytes Sent	Bytes sent through the VPN connection.
Disconnect	Select to disconnect the VPN connection.

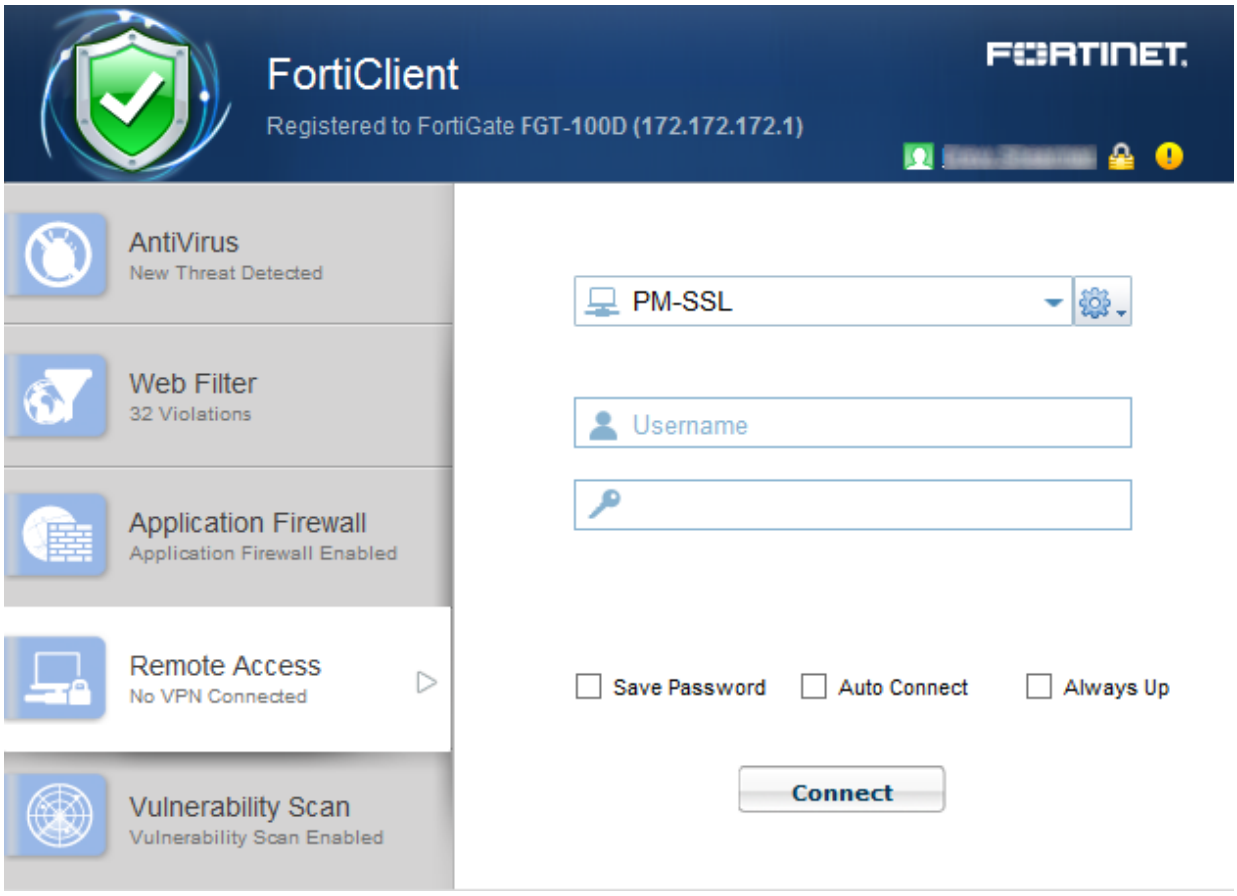
Save Password, Auto Connect, and Always Up (Keep Alive)

When configuring a FortiClient VPN (IPsec) or SSL VPN connection on your FortiGate device, you can select to enable the following features:

- *Save Password*: Allows the user to save the VPN connection password in the console.
- *Auto Connect*: When FortiClient is launched, the VPN connection will automatically connect.
- *Always Up (Keep Alive)*: When selected, the VPN connection is always up even when no data is being processed. If the connection fails, keep alive packets sent to the FortiGate will sense when the VPN connection is available and re-connect.

For SSL VPN tunnel mode configurations these features are enabled/disabled in the *SSL VPN Portal*.

When enabled in the FortiGate configuration, once the FortiClient is connected to the FortiGate, the client will receive these configuration options.



For FortiClient VPN configurations, once these features are enabled they may only be edited from the command line. Use the following FortiOS CLI commands to disable these features:

```
config vpn ipsec phase1-interface
   edit [vpn name]
      set save-password disable
```

```
        set client-auto-negotiate disable
        set client-keep-alive disable
    end
end
```

FortiToken and FortiClient VPN

You can use FortiToken with FortiClient for two-factor authentication. See the *FortiOS 5.0 Handbook* for information on configuring FortiToken, user groups, VPN, and two-factor authentication on your FortiGate device for FortiClient VPN connections.

Advanced features (Microsoft Windows)

When deploying a custom FortiClient XML configuration, use the advanced FortiClient Profile options in FortiGate to ensure the FortiClient Profile settings do not overwrite your custom XML settings. For more information, see the *FortiClient XML Reference* and the *CLI Reference for FortiOS*.

Activating VPN before Windows Logon

When using VPN before Windows logon, the user is offered a list of pre-configured VPN connections to select from on the Windows logon screen. This requires that the Windows logon screen is not bypassed. As such, if VPN

before Windows logon is enabled, it is required to also check the check box *Users must enter a user name and password to use this computer* in the *User Accounts* dialog box.

To make this change, proceed as follows:

In FortiClient,

1. Create the VPN tunnels of interest or use Endpoint Control to register to a FortiGate which provides the VPN list of interest
2. Enable VPN before logon on the FortiClient Settings page, see VPN options on page 130.

On the Microsoft Windows system,

1. Start an elevated command line prompt.
2. Enter `control passwords2` and press `Enter`. Alternatively, you can enter `netplwiz`.
3. Check the check box for *Users must enter a user name and password to use this computer*.
4. Click *OK* to save the setting.

Connect VPN before logon (AD environments)

The VPN `<options>` tag holds global information controlling VPN states. The VPN will connect first, then logon to AD/Domain.

```
<forticlient_configuration>
   <vpn>
      <options>
         <show_vpn_before_logon>1</show_vpn_before_logon>
         <use_windows_credentials>1</use_windows_credentials>
      </options>
   </vpn>
</forticlient_configuration>
```

Create a redundant IPsec VPN

To use VPN resiliency/redundancy, you will configure a list of FortiGate IP/FQDN servers, instead of just one:

```
<forticlient_configuration>
   <vpn>
      <ipsecvpn>
            <options>
            ...
            </options>
               <connections>
                  <connection>
                     <name>psk_90_1</name>
                     <type>manual</type>
                     <ike_settings>
                     <prompt_certificate>0</prompt_certificate>
                     <server>10.10.90.1;ipsecdemo.fortinet.com;172.17.61.143</server>
                     <redundantsortmethod>1</redundantsortmethod>
                     ...
               </ike_settings>
            </connection>
         </connections>
      </ipsecvpn>
   </vpn>
</forticlient_configuration>
```

This is a balanced, but incomplete XML configuration fragment. All closing tags are included, but some important elements to complete the IPsec VPN configuration are omitted.

RedundantSortMethod = 1

This XML tag sets the IPsec VPN connection as ping-response based. The VPN will connect to the FortiGate which responds the fastest.

RedundantSortMethod = 0

By default, RedundantSortMethod =0 and the IPsec VPN connection is priority based. Priority based configurations will try to connect to the FortiGate starting with the first in the list.

Priority based SSL VPN connections

SSL VPN supports priority based configurations for redundancy.

```
<forticlient_configuration>
   <vpn>
      <sslvpn>
         <options>
            <enabled>1</enabled>
            ...
         </options>
         <connections>
            <connection>
               <name>ssl_90_1</name>
               <server>10.10.90.1;ssldemo.fortinet.com;172.17.61.143:443</server>
               ...
            </connection>
         </connections>
      </sslvpn>
   </vpn>
</forticlient_configuration>
```

This is a balanced, but incomplete XML configuration fragment. All closing tags are included, but some important elements to complete the SSL VPN configuration are omitted.

For SSL VPN, all FortiGates must use the same TCP port.

Advanced features (Mac OS X)

When deploying a custom FortiClient XML configuration, use the advanced FortiClient Profile options in FortiGate to ensure the FortiClient Profile settings do not overwrite your custom XML settings. For more information, see the *FortiClient XML Reference* and the *CLI Reference for FortiOS*.

Create a redundant IPsec VPN

To use VPN resiliency/redundancy, you will configure a list of FortiGate IP/FQDN servers, instead of just one:

```
<forticlient_configuration>
   <vpn>
```

```
<ipsecvpn>
     <options>
     ...
     </options>
        <connections>
           <connection>
              <name>psk_90_1</name>
              <type>manual</type>
              <ike_settings>
              <prompt_certificate>0</prompt_certificate>
              <server>10.10.90.1;ipsecdemo.fortinet.com;172.17.61.143</server>
              <redundantsortmethod>1</redundantsortmethod>
              ...
           </ike_settings>
        </connection>
     </connections>
  </ipsecvpn>
</vpn>
</forticlient_configuration>
```

This is a balanced, but incomplete XML configuration fragment. All closing tags are included, but some important elements to complete the IPsec VPN configuration are omitted.

RedundantSortMethod = 1

This XML tag sets the IPsec VPN connection as ping-response based. The VPN will connect to the FortiGate which responds the fastest.

RedundantSortMethod = 0

By default, RedundantSortMethod =0 and the IPsec VPN connection is priority based. Priority based configurations will try to connect to the FortiGate starting with the first in the list.

Priority based SSL VPN connections

SSL VPN supports priority based configurations for redundancy.

```
<forticlient_configuration>
  <vpn>
     <sslvpn>
        <options>
           <enabled>1</enabled>
           ...
        </options>
        <connections>
           <connection>
              <name>ssl_90_1</name>
              <server>10.10.90.1;ssldemo.fortinet.com;172.17.61.143:443</server>
              ...
           </connection>
        </connections>
     </sslvpn>
  </vpn>
</forticlient_configuration>
```

This is a balanced, but incomplete XML configuration fragment. All closing tags are included, but some important elements to complete the SSL VPN configuration are omitted.

For SSL VPN, all FortiGates must use the same TCP port.

VPN tunnel & script (Microsoft Windows)

When deploying a custom FortiClient XML configuration, use the advanced FortiClient Profile options in FortiGate to ensure the FortiClient Profile settings do not overwrite your custom XML settings. For more information, see the *FortiClient XML Reference* and the *CLI Reference for FortiOS*.

Feature overview

This feature supports auto running a user-defined script after the configured VPN tunnel is connected or disconnected. The scripts are batch scripts in Windows and shell scripts in Mac OS X. They are defined as part of a VPN tunnel configuration on FortiGate's XML format FortiClient Profile. The profile will be pushed down to FortiClient from FortiGate. When FortiClient's VPN tunnel is connected or disconnected, the respective script defined under that tunnel will be executed.

Map a network drive after tunnel connection

The script will map a network drive and copy some files after the tunnel is connected.

```
<on_connect>
   <script>
      <os>windows</os>
         <script>
            <script>
               <![CDATA[
net use x: \\192.168.10.3\ftpshare /user:Ted Mosby
md c:\test
copy x:\PDF\*.* c:\test
                  ]]>
            </script>
         </script>
      </script>
   </on_connect>
```

Delete a network drive after tunnel is disconnected

The script will delete the network drive after the tunnel is disconnected.

```
<on_disconnect>
   <script>
      <os>windows</os>
      <script>
         <script>
            <![CDATA[
net use x: /DELETE
               ]]>
</script>
         </script>
      </script>
```

```
</on_disconnect>
```

VPN tunnel & script (Mac OS X)

When deploying a custom FortiClient XML configuration, use the advanced FortiClient Profile options in FortiGate to ensure the FortiClient Profile settings do not overwrite your custom XML settings. For more information, see the *FortiClient XML Reference* and the *CLI Reference for FortiOS*.

Map a network drive after tunnel connection

The script will map a network drive and copy some files after the tunnel is connected.

```
<on_connect>
   <script>
      <os>mac</os>
      <script>
         /bin/mkdir /Volumes/installers
         /sbin/ping -c 4 192.168.1.147 > /Users/admin/Desktop/dropbox/p.txt
         /sbin/mount -t smbfs //kimberly:RigUpTown@ssldemo.fortinet.com/installers
             /Volumes/installers/ > /Users/admin/Desktop/dropbox/m.txt
         /bin/mkdir /Users/admin/Desktop/dropbox/dir
         /bin/cp /Volumes/installers/*.log /Users/admin/Desktop/dropbox/dir/.
      </script>
   </script>
</on_connect>
```

Delete a network drive after tunnel is disconnected

The script will delete the network drive after the tunnel is disconnected.

```
<on_disconnect>
   <script>
      <os>mac</os>
      <script>
         /sbin/umount /Volumes/installers
         /bin/rm -fr /Users/admin/Desktop/dropbox/*
   </script>
   </script>
</on_disconnect>
```

Vulnerability Scan

FortiClient includes an *Vulnerability Scan* module to check your workstation for known system vulnerabilities. You can scan on-demand or on a scheduled basis. This feature is disabled by default and the tab is hidden for standalone clients. For users who are registered to a FortiGate using endpoint control, the FortiGate administrator may choose to enable this feature. Vulnerability Scan is enabled via the FortiGate Command Line Interface (CLI) only. Once enabled, the *Endpoint Vulnerability Scan on Client* setting is available in the FortiClient Profile.

Enable Vulnerability Scan

This section describes how to enable *Vulnerability Scan* in the FortiClient Profile via the FortiGate CLI and configuration options.

1. Enable Vulnerability Scan in the FortiClient Profile:
2. Login to your FortiGate CLI.
3. Enter the following CLI commands:

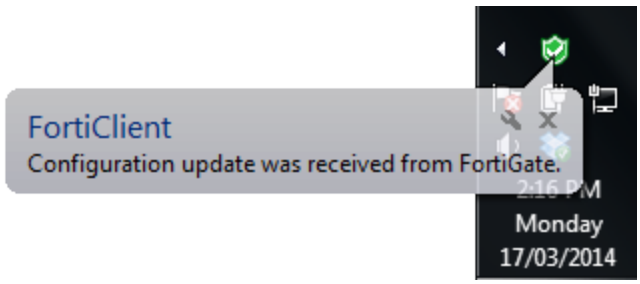
```
config endpoint-control profile
   edit <profile-name>
      config forticlient-winmac-settings
         set forticlient-vuln-scan enable
         set forticlient-vuln-scan-schedule {daily | weekly | monthly}
         set forticlient-vuln-scan-on-registration {enable | disable}
         set forticlient-ui-options {av | wf | af | vpn | vs}
      end
   end
```

When setting the `forticlient-ui-options`, you must include all the modules that you want to enable in the FortiClient console.

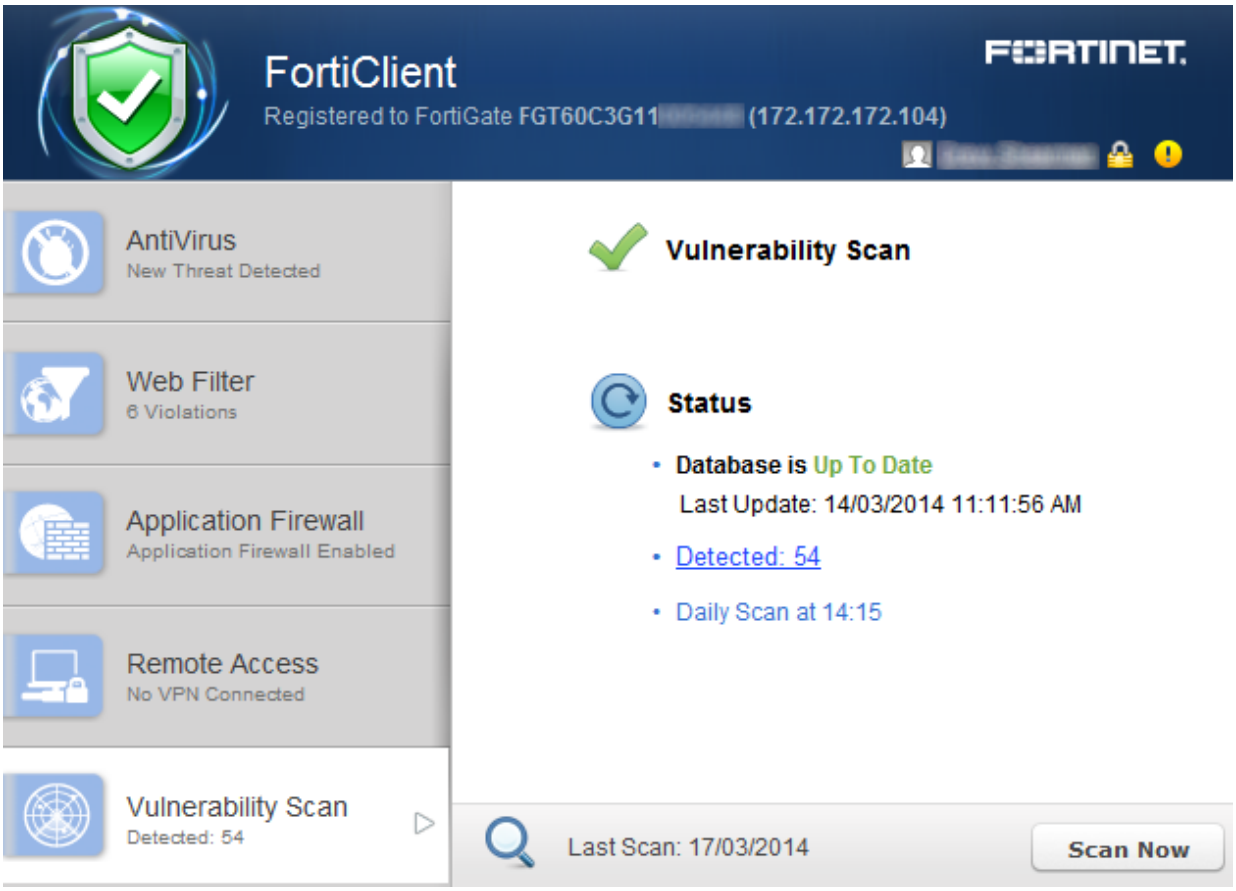
`<profile-name>`	Enter the name of the FortiClient Profile.
`forticlient-vuln-scan {enable | disable}`	Enable or disable the Vulnerability Scan module.
`forticlient-vuln-scan-schedule {daily | weekly | monthly}`	Configure a daily, weekly, or monthly vulnerability scan on the client workstation.

`forticlient-vuln-scan-on-registration {enable | disable}`	Enable or disable vulnerability scan on client registration to FortiGate.
`forticlient-ui-options {av | wf | af | vpn | vs}`	Set the FortiClient components that will be available to the client upon registration with FortiGate. • av: AntiVirus • wf: Web Filter • af: Application Firewall • vpn: Remote Access • vs: Vulnerability Scan

4. The FortiGate will send the FortiClient Profile configuration update to registered clients.



The Vulnerability Scan module is now available in FortiClient.



Scan now

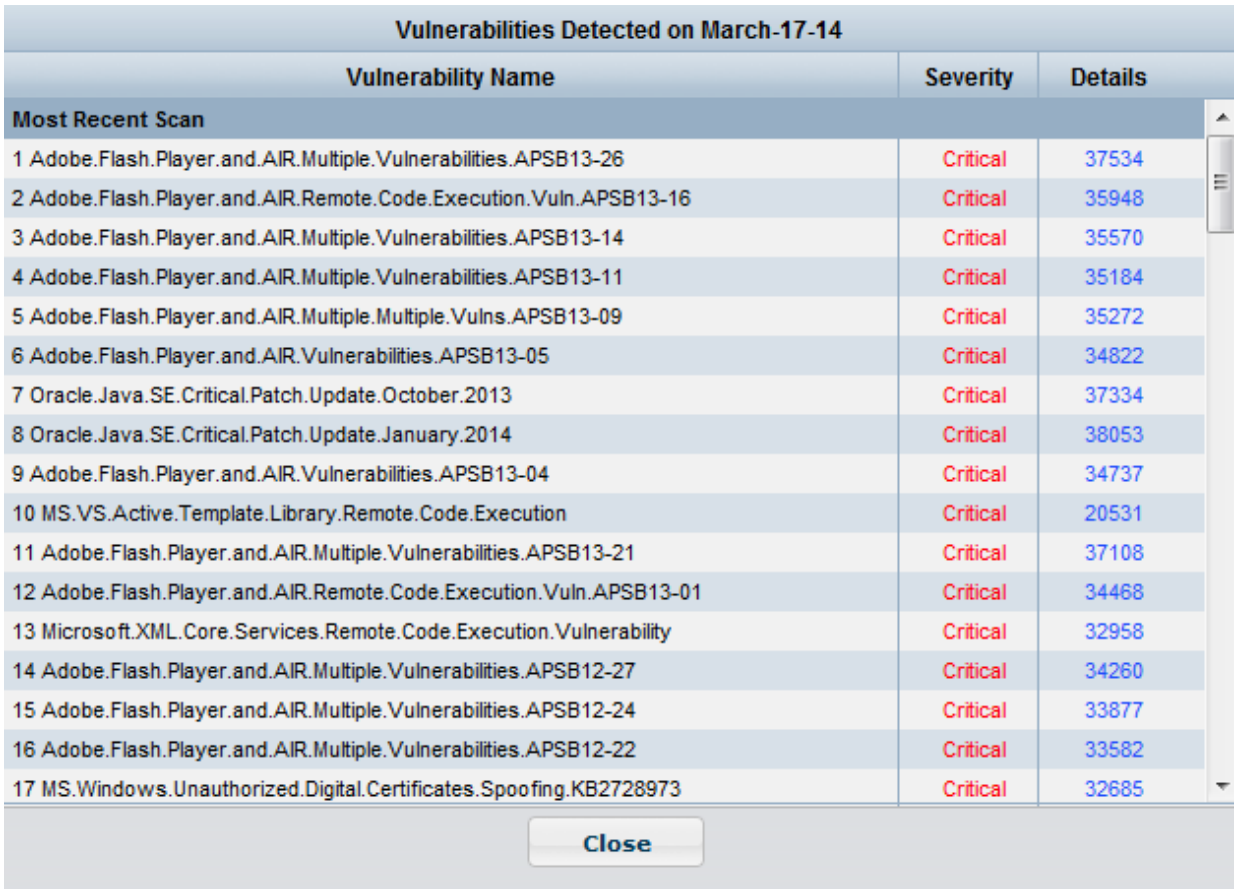
To perform a vulnerability scan, select the *Scan Now* button in the FortiClient console. FortiClient will scan your workstation for known vulnerabilities. The console displays the date of the last scan above the button.

You can select to use a FortiManager device for client software and signature updates. When configuring the FortiClient Profile, select *Use FortiManager for client software/signature update* to enable the feature and enter the IP address of your FortiManager device.

View vulnerabilities

When the scan is complete, FortiClient will display the number of vulnerabilities found in the FortiClient console.

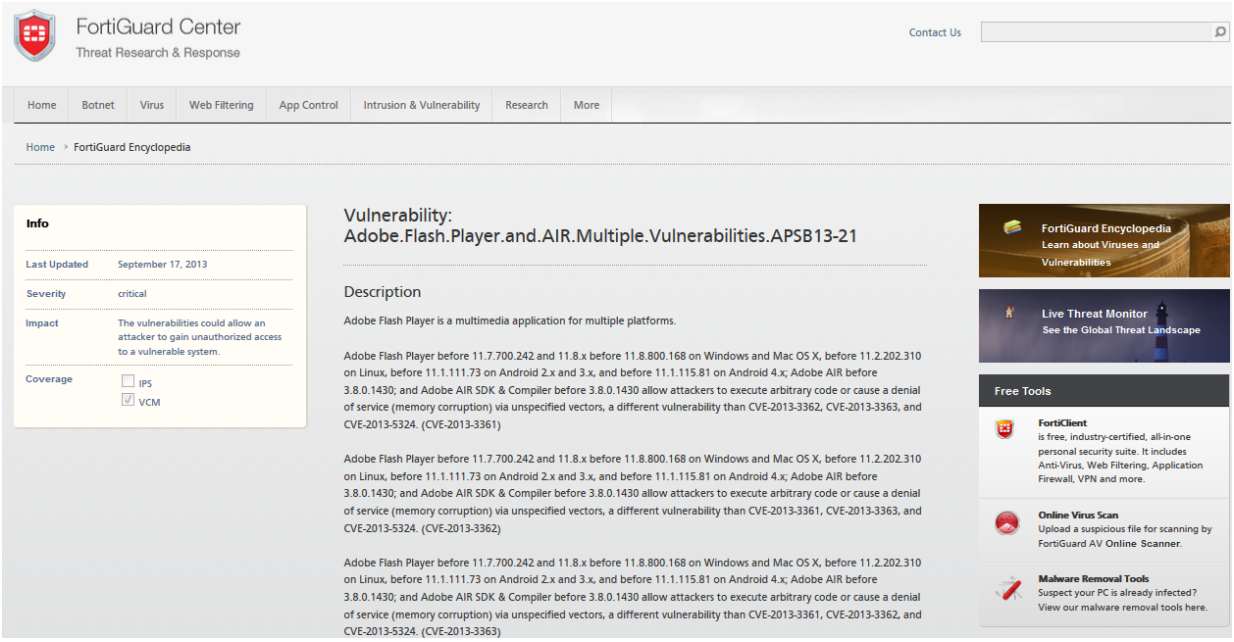
Select the *Vulnerabilities Detected* link to view a list of vulnerabilities detected on your system.



This page displays the following:

Vulnerability Name	The name of the vulnerability
Severity	The severity level assigned to the vulnerability; Critical, High, Medium, Low, Info.
Details	FortiClient vulnerability scan lists a Bugtraq (BID) number under the details column. You can select the BID to view details of the vulnerability on the FortiGuard site, or search the web using this BID number.
Close	Close the window and return to the FortiClient console.

Select the *Details* ID number from the list to view information on the selected vulnerability on the FortiGuard site. The site details the release date, severity, impact, description, affected products, and recommended actions.


FortiGuard Center
Threat Research & Response
Contact Us
Home
Botnet
Virus
Web Filtering
App Control
Intrusion & Vulnerability
Research
More
Home › FortiGuard Encyclopedia
Info
Last Updated
September 17, 2013
Severity
critical
Impact
The vulnerabilities could allow an attacker to gain unauthorized access to a vulnerable system.
Coverage
IPS
VCM
Vulnerability:
Adobe.Flash.Player.and.AIR.Multiple.Vulnerabilities.APSB13-21
Description
Adobe Flash Player is a multimedia application for multiple platforms.
Adobe Flash Player before 11.7.700.242 and 11.8.x before 11.8.800.168 on Windows and Mac OS X, before 11.2.202.310 on Linux, before 11.1.111.73 on Android 2.x and 3.x, and before 11.1.115.81 on Android 4.x; Adobe AIR before 3.8.0.1430; and Adobe AIR SDK & Compiler before 3.8.0.1430 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-3362, CVE-2013-3363, and CVE-2013-5324. (CVE-2013-3361)
Adobe Flash Player before 11.7.700.242 and 11.8.x before 11.8.800.168 on Windows and Mac OS X, before 11.2.202.310 on Linux, before 11.1.111.73 on Android 2.x and 3.x, and before 11.1.115.81 on Android 4.x; Adobe AIR before 3.8.0.1430; and Adobe AIR SDK & Compiler before 3.8.0.1430 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-3361, CVE-2013-3363, and CVE-2013-5324. (CVE-2013-3362)
Adobe Flash Player before 11.7.700.242 and 11.8.x before 11.8.800.168 on Windows and Mac OS X, before 11.2.202.310 on Linux, before 11.1.111.73 on Android 2.x and 3.x, and before 11.1.115.81 on Android 4.x; Adobe AIR before 3.8.0.1430; and Adobe AIR SDK & Compiler before 3.8.0.1430 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-3361, CVE-2013-3362, and CVE-2013-5324. (CVE-2013-3363)
FortiGuard Encyclopedia
Learn about Viruses and Vulnerabilities
Live Threat Monitor
See the Global Threat Landscape
Free Tools
FortiClient
is free, industry-certified, all-in-one personal security suite. It includes Anti-Virus, Web Filtering, Application Firewall, VPN and more.
Online Virus Scan
Upload a suspicious file for scanning by FortiGuard AV Online Scanner.
Malware Removal Tools
Suspect your PC is already infected? View our malware removal tools here.

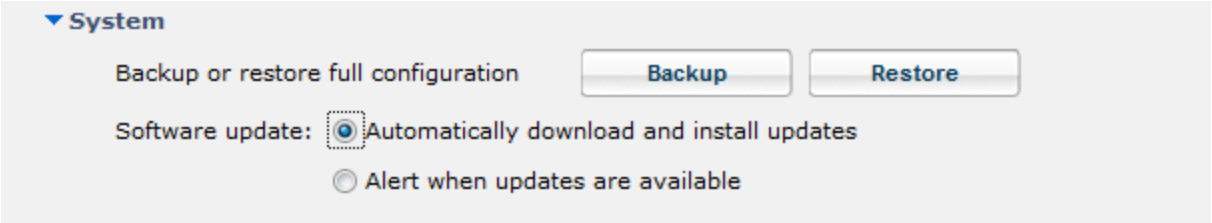
Settings

This sections describe the available options in the settings menu.

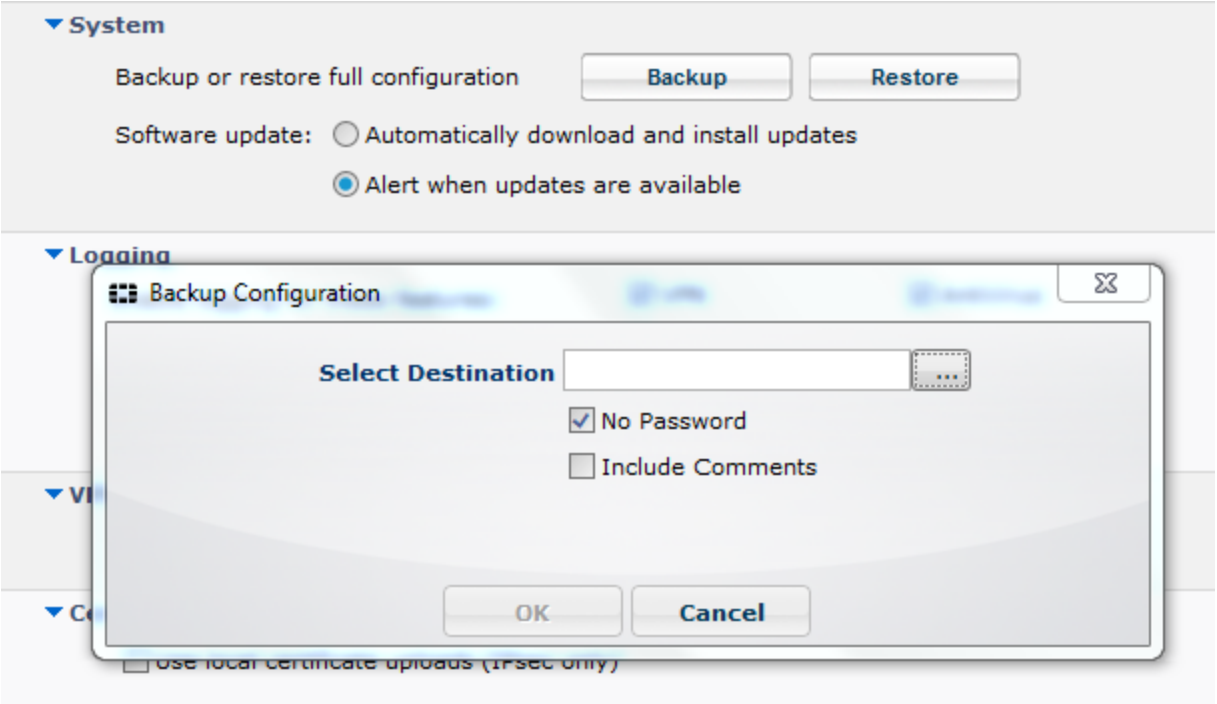
Backup or restore full configuration

To backup or restore the full configuration file select *File* in the toolbar and select *Settings* in the drop-down menu. Select *System* to view the drop-down menu. In this menu you can perform a backup or restore a full configuration file.

Backup	Backup is available when in standalone mode or when registered to FortiGate.
Restore	Restore is available when in standalone mode.

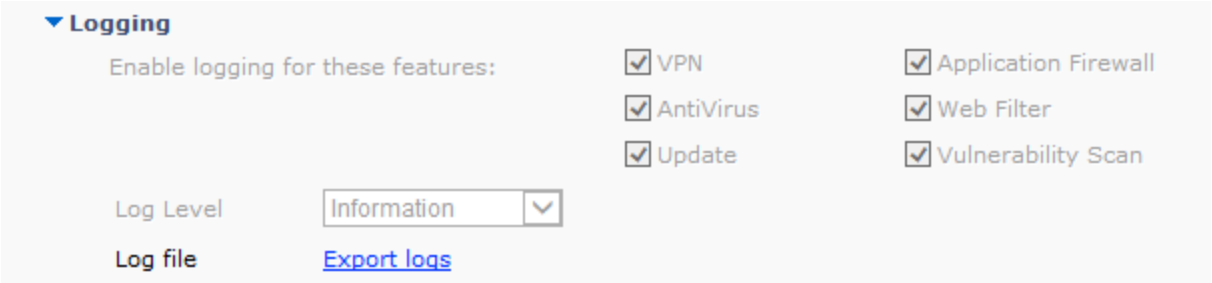


When performing a backup you can select the file destination and save the file in an unencrypted (`.conf`) or encrypted format (`.sconf`). You can select to include or exclude comments in the XML configuration file.



Logging

To configure logging, select *File* in the toolbar and select *Settings* in the drop-down menu. Select *Logging* to view the drop-down menu. You can specify the logging level and select to export logs or clear logs.



VPN	VPN logging is available when in standalone mode or when registered to FortiGate.
Application Firewall	Application Firewall logging is available when registered to FortiGate.
AntiVirus	Antivirus activity logging is available when in standalone mode or when registered to FortiGate.
Web Filter	Web Filter logging is available when in standalone mode (Web Security) or when registered to FortiGate.
Update	Update logging is available when in standalone mode or when registered to FortiGate.
Vulnerability Scan	Vulnerability Scan logging is available when registered to FortiGate.
Log Level	This setting can be configured when in standalone mode. When registered to FortiGate, this setting is set by the XML configuration (if configured).
Log File	The option to export the log file (`.log`) is available when in standalone mode or when registered to FortiGate. The option to clear logs is only available when in standalone mode.

The following table lists the logging levels and description:

Logging Level	Description
Emergency	The system becomes unstable.
Alert	Immediate action is required.
Critical	Functionality is affected.

Logging Level	Description
Error	An error condition exists and functionality could be affected.
Warning	Functionality could be affected.
Notice	Information about normal events.
Information	General information about system operations.
Debug	Debug FortiClient.

FortiClient can be configured via the endpoint profile to send traffic, vulnerability scan, and event logs to your FortiAnalyzer or FortiManager device running v5.0.2 or later.

Configure logging to FortiAnalyzer or FortiManager

To configure FortiClient to log to your FortiAnalyzer or FortiManager you require the following:

- FortiClient v5.2.0 or later
- A FortiGate device running FortiOS v5.2.0 or later
- A FortiAnalyzer or FortiManager device running v5.0.7 or later

The registered FortiClient device will send traffic logs, vulnerability scan logs, and event logs to the log device on port 514 TCP.

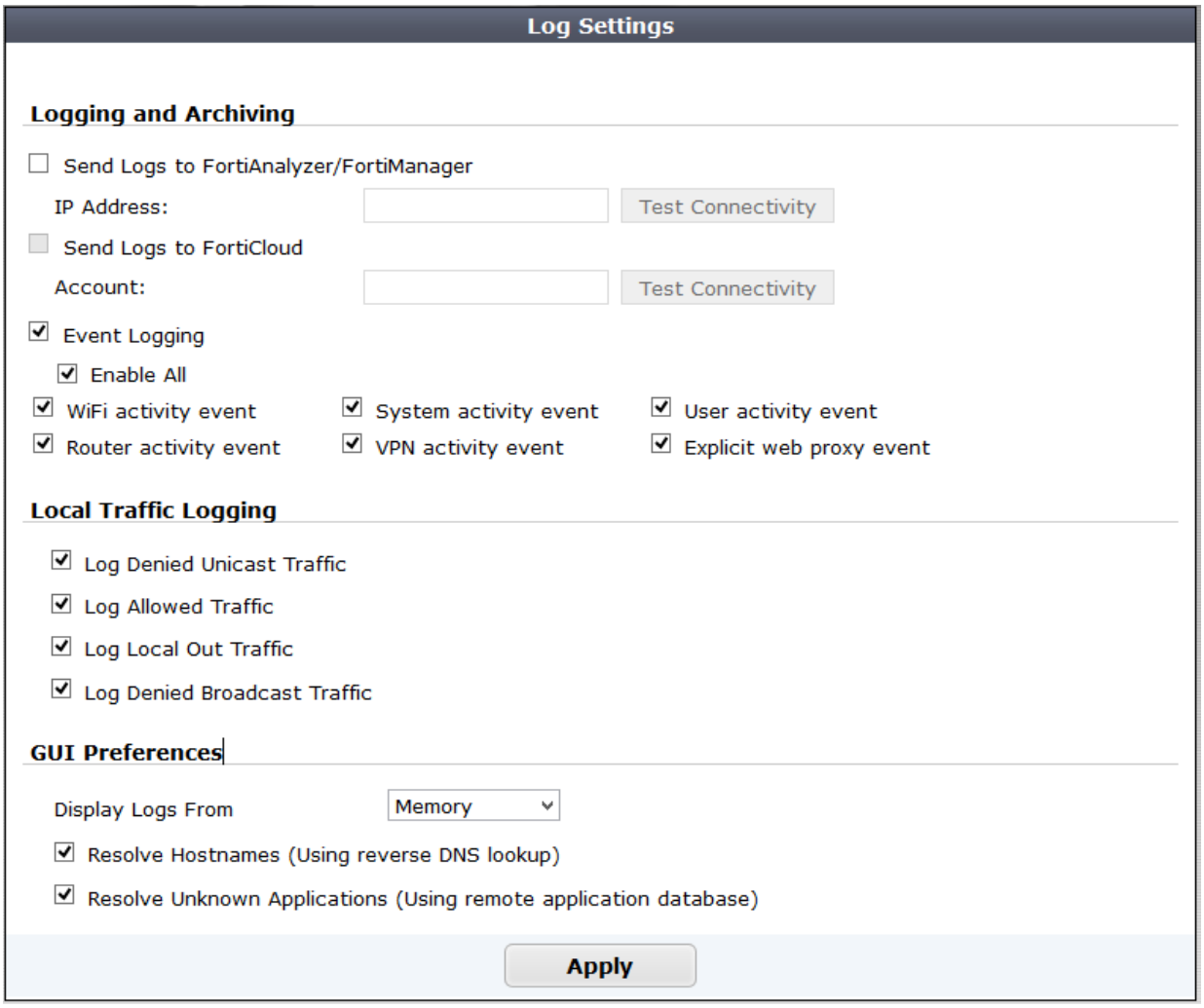
FortiClient must be registered to FortiGate to upload logs to FortiAnalyzer/FortiManager.

When FortiClient is On-Net, the icon displayed to the left of the username will be green. When FortiClient is Off-Net, the icon is grey.

Some features such as Client-based Logging when On-Net, are only available in the FortiClient Profile when a FortiClient v5.2 license has been applied to the FortiGate.

Enable logging on the FortiGate device:

1. On your FortiGate device, select *Log & Report* > *Log Config* > *Log Settings*. The *Log Settings* window opens.

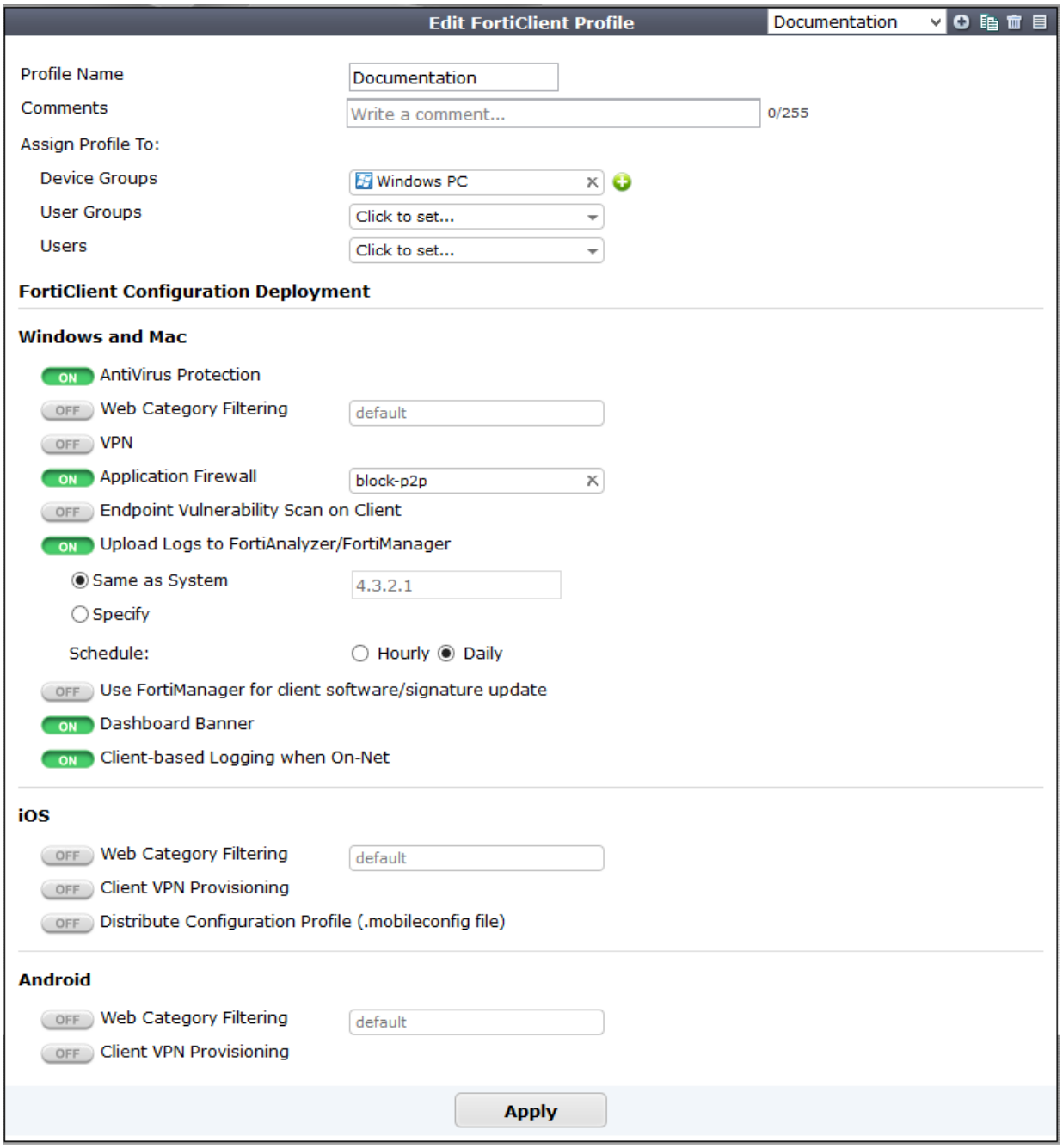


2. Select the *Send Logs to FortiAnalyzer/FortiManager* checkbox to enable this feature. Enter the IP address of your log device. You can select *Test Connectivity* to ensure your FortiGate is able to communicate with the log device on this IP address.
3. Select *Apply* to save the setting.

FortiClient must be able to access the FortiAnalyzer IP address in order to forward logs.

Enable logging in the FortiClient Profile:

1. Go to *User & Device* > *FortiClient Profiles*.
2. Select the FortiClient Profile and select *Edit* from the toolbar. The *Edit FortiClient Profile* page opens.



3. In the FortiClient Configuration Deployment Windows and Mac section, toggle the *Upload Logs to FortiAnalyzer/FortiManager* feature to *ON*. You can select either *Same as System* which will follow the FortiGate settings or *Specify* to enter a different IP address. For *Schedule*, select to upload logs *Hourly* or *Daily*.
4. Select Apply to save the setting. Once the FortiClient Profile change is synchronized with the client, you will start receiving logs from registered clients on your FortiAnalyzer/FortiManager system.

   Alternatively, you can configure logging in the command line interface. Go to *System* > *Dashboard* > *Status*. In the CLI Console widget, enter the following CLI commands:

```
config endpoint-control profile
  edit <profile-name>
  config forticlient-winmac-settings
```

```
            set forticlient-log-upload enable
            set forticlient-log-upload-server <IP address>
            set forticlient-log-upload-schedule {hourly | daily}
            set forticlient-log-ssl-upload {enable | disable}
            set client-log-when-on-net {enable | disable}
        end
    end
```

To download the FortiClient log files on the FortiAnalyzer go to the *Log View* tab, select the ADOM, and select the *FortiClient* menu object.

Updates

To configure updates, select *File* in the toolbar and select *Settings* in the drop-down menu. Select *System* to view the drop-down menu. In this menu you can configure the behavior of FortiClient when a new software version is available on the FortiGuard Distribution Servers (FDS).

Software update	This setting can be configured when in standalone mode. When registered to FortiGate, this setting is set by the XML configuration (if configured).

You can select to use a FortiManager device for signature updates. When configuring the endpoint profile, select *Use FortiManager for client software/signature updates* to enable the feature and enter the IP address of your FortiManager device.

To configure FortiClient to use FortiManager for signature updates:

1. On your FortiOS device, select *User & Device* > *FortiClient Profiles*.
2. Toggle the *Use FortiManager for client software/signature update* option to *ON*.
3. Specify the IP address of the FortiManager to use for signature updates.
4. Select the checkbox beside *Failover to FDN when FortiManager is not available* to have FortiClient receive updates from the FortiGuard Distribution Network when the FortiManager is not available to ensure your clients are always protected.
5. Select *Apply* to save the setting.

VPN options

To configure VPN options, select *File* in the toolbar and select *Settings* in the drop-down menu. Select *VPN Options* to view the drop-down menu. In this menu you can configure to enable VPN before logon.

This setting can be configured when in standalone mode. When registered to FortiGate, this setting is set by the XML configuration (if configured).

Certificate management

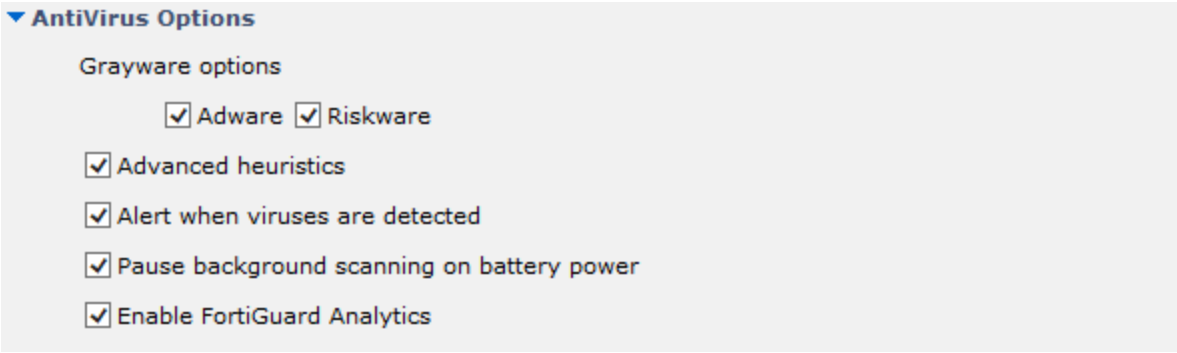
To configure VPN certificates, select *File* in the toolbar and select *Settings* in the drop-down menu. Select *Certificate Management* to view the drop-down menu. In this menu you can configure IPsec VPN to use local certificates and import certificates to FortiClient.

This setting can be configured when in standalone mode. When registered to FortiGate, this setting is set by the XML configuration (if configured).

Antivirus options

To configure antivirus options, select *File* in the toolbar and select *Settings* in the drop-down menu. Select *AntiVirus Options* to view the drop-down menu. In this menu you can configure grayware options and the behavior of FortiClient when a virus is detected.

These settings can be configured when in standalone mode. When registered to FortiGate, these settings are set by the XML configuration (if configured).



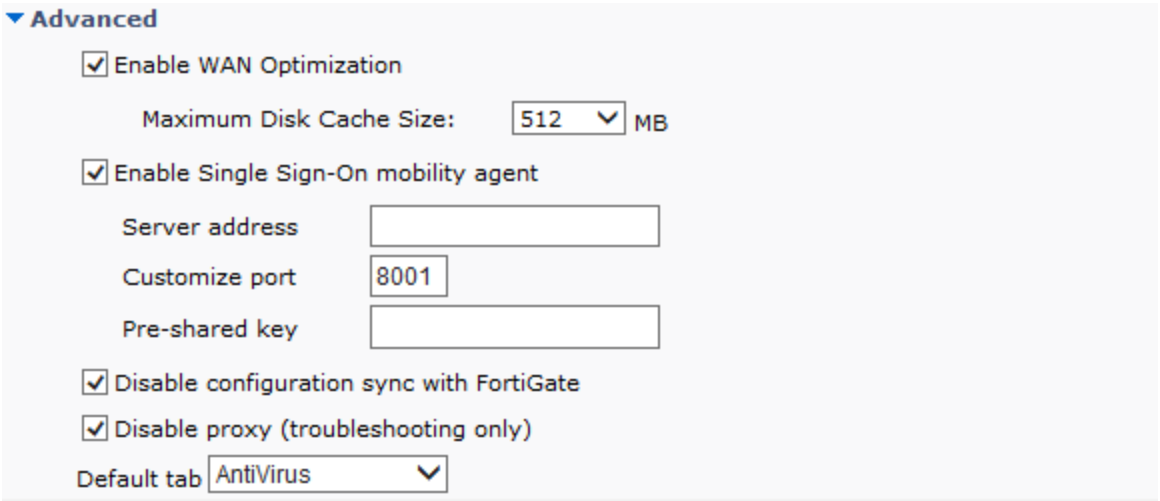
Configure the following settings:

Grayware Options	Grayware is an umbrella term applied to a wide range of malicious applications such as spyware, adware and key loggers that are often secretly installed on a user's computer to track and/or report certain information back to an external source without the user's permission or knowledge.
Adware	Select to enable adware detection and quarantine during the antivirus scan.
Riskware	Select to enable riskware detection and quarantine during the antivirus scan.
Advanced heuristics	Select to enable advanced heuristics.
Alert when viruses are detected	Select to display notification message window when a virus is detected.

Pause background scanning on battery power	Select to pause background scanning when on battery power.
Enable FortiGuard Analytics	Select to automatically send suspicious files to the FortiGuard Network for analysis.

Advanced options

To configure advanced options, select *File* in the toolbar, and select *Settings* in the drop-down menu. Select *Advanced* to view the drop-down menu. In this menu you can configure WAN Optimization, Single Sign-On, configuration sync with FortiGate, disable proxy, and the default tab when FortiClient is started.



Configure the following settings:

Advanced	Advanced FortiClient settings.
Enable WAN Optimization	Select to enable WAN Optimization. You should enable only if you have a FortiGate device and your FortiGate is configured for WAN Optimization. This setting can be configured when in standalone mode. When registered to FortiGate, this setting is set by the XML configuration (if configured).
Maximum Disk Cache Size	Select to configure the maximum disk cache size. The default value is 512MB.
Enable Single Sign-On mobility agent	Select to enable Single Sign-On Mobility Agent for FortiAuthenticator. To use this feature you need to apply a FortiClient SSO mobility agent license to your FortiAuthenticator device. This setting can be configured when in standalone mode. When registered to FortiGate, this setting is set by the XML configuration (if configured).
Server address	Enter the FortiAuthenticator IP address.

Customize port	Enter the port number. The default port is 8001.
Pre-shared Key	Enter the pre-shared key. The pre-shared key should match the key configured on your FortiAuthenticator device.
Disable configuration sync with FortiGate	Select to disable configuration synchronization with FortiGate. By disabling this option, this client will be considered as non-compliant and your network traffic might be blocked by FortiGate. This setting can be configured when in standalone mode or when registered to FortiGate.
Disable proxy (troubleshooting only)	Select to disable proxy when troubleshooting FortiClient. This setting can be configured when in standalone mode. When registered to FortiGate, this setting is set by the XML configuration (if configured).
Default tab	Select the default tab to be displayed when opening FortiClient. This setting can be configured when in standalone mode. When registered to FortiGate, this setting is set by the XML configuration (if configured).

Single Sign-On (SSO) mobility agent

The FortiClient Single Sign-On Mobility Agent is a client that updates with FortiAuthenticator with user logon and network information.

FortiClient/FortiAuthenticator protocol

The FortiAuthenticator listens on a configurable TCP port. FortiClient connects to FortiAuthenticator using TLS/SSL with two-way certificate authentication. The FortiClient sends a logon packet to FortiAuthenticator, which replies with an acknowledgement packet.

FortiClient/FortiAuthenticator communication requires the following:

- The IP address should be unique in the entire network.
- The FortiAuthenticator should be accessible from clients in all locations.
- The FortiAuthenticator should be accessible by all FortiGates.

FortiClient Single Sign-On Mobility Agent requires a FortiAuthenticator running v2.0.0 or later, or v3.0.0 or later. Enter the FortiAuthenticator (server) IP address, port number, and the pre-shared key configured on the FortiAuthenticator.

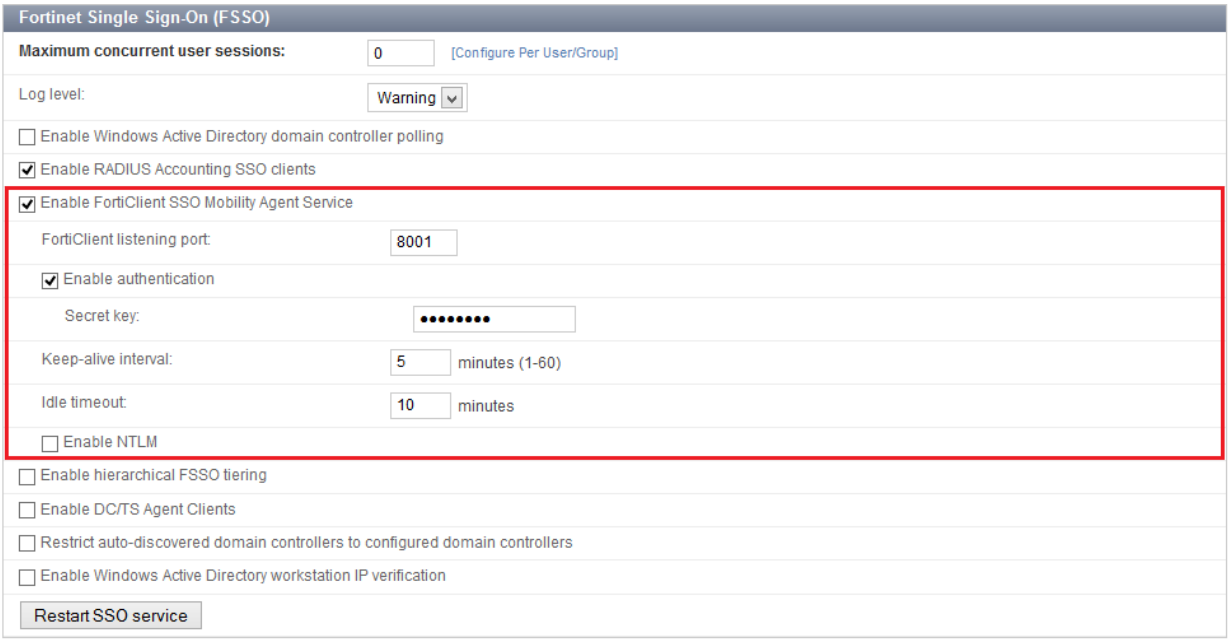
Enable Single Sign-On mobility agent on FortiClient:

1. Select *File* in the toolbar and select *Settings* in the drop-down menu.
2. Select *Advanced* to view the drop-down menu.
3. Select to *Enable Single Sign-On mobility agent*.
4. Enter the FortiAuthenticator server address and the pre-shared key.

This setting can be configured when in standalone mode. When registered to FortiGate, this setting is set by the XML configuration (if configured).

Enable FortiClient SSO mobility agent service on the FortiAuthenticator:

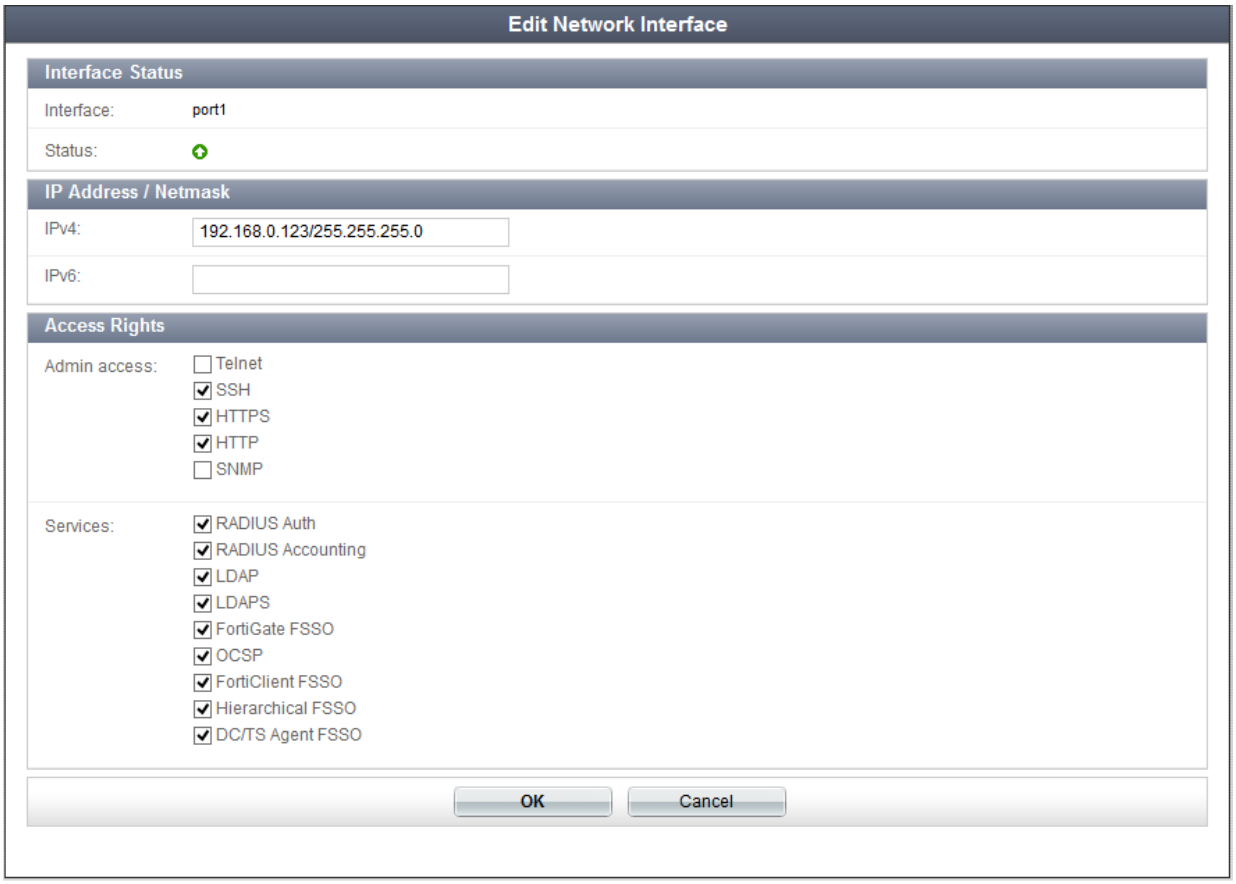
1. Select *Fortinet SSO Methods* > *SSO* > *General*. The *Edit SSO Configuration* page opens.



2. Select *Enable FortiClient SSO Mobility Agent Service* and a TCP port value for the listening port.
3. Select *Enable authentication* and enter a secret-key value.
4. Select *OK* to save the setting.

To enable FortiClient FSSO services on the interface:

1. Select *System* > *Network* > *Interfaces*. Select the interface and select Edit from the toolbar. The *Edit Network Interface* window opens.

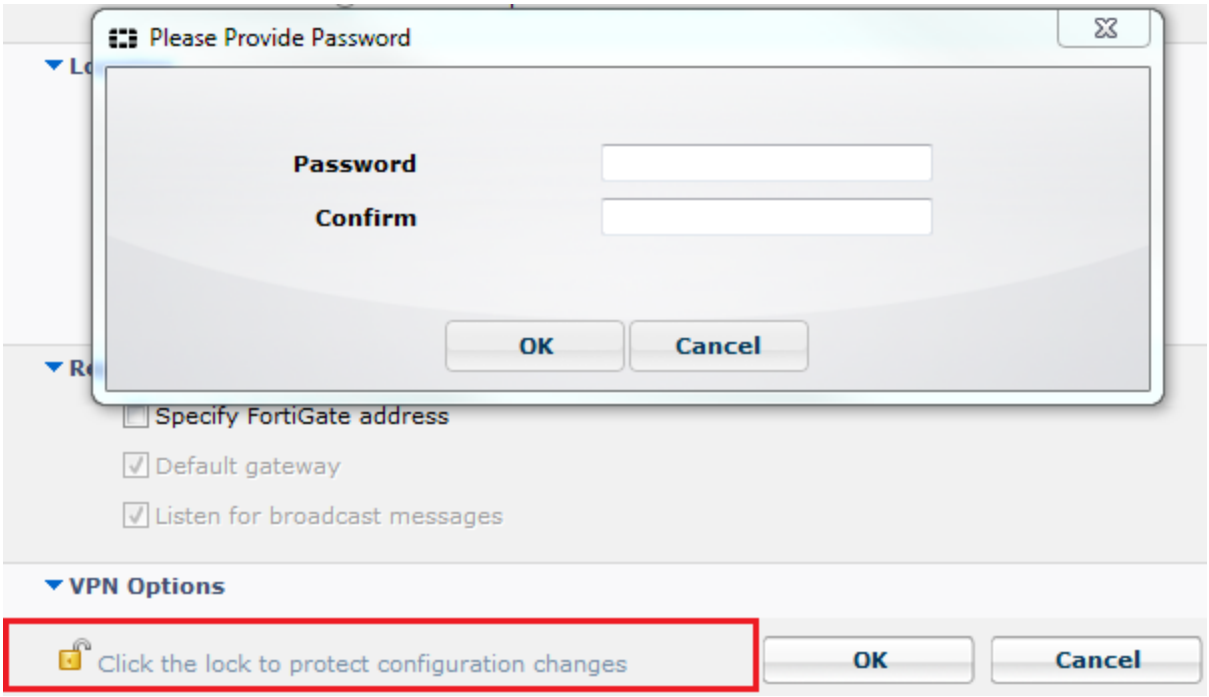


2. Select the checkbox to enable *FortiClient FSSO*.
3. Select *OK* to save the setting.

To enable the FortiClient SSO Mobility Agent Service on the FortiAuthenticator, you must first apply the applicable FortiClient license for FortiAuthenticator. For more information, see the *FortiAuthenticator Administration Guide* in the Fortinet Document Library at http://docs.fortinet.com. For information on purchasing a FortiClient license for FortiAuthenticator, please contact your authorized Fortinet reseller.

Configuration lock

To prevent unauthorized changes to the FortiClient configuration, select the lock icon located at the bottom left of the *Settings* page. You will be prompted to enter and confirm a password. When the configuration is locked, configuration changes are restricted and FortiClient cannot be shut down or uninstalled.



When the configuration is locked you can perform the following actions:

- Antivirus:
  - Complete an antivirus scan, view threats found, and view logs
  - Select *Update Now* to update signatures
- Web Security
- Antivirus:
  - View violations
- Application Firewall
  - View applications blocked
- Remote Access
  - Configure, edit, or delete an IPsec VPN or SSL VPN connection
  - Connect to a VPN connection
- Vulnerability Scan
  - Complete a vulnerability scan of the system
  - View vulnerabilities found
- Register and unregister FortiClient for Endpoint Control
- Settings
  - Export FortiClient logs
  - Backup the FortiClient configuration

To perform configuration changes or to shut down FortiClient, select the lock icon and enter the password used to lock the configuration.

FortiTray

When FortiClient is running on your system, you can select the FortiTray icon in the Windows system tray to perform various actions. The FortiTray icon is available in the system tray even when the FortiClient console is closed.

- Default menu options
  - Open FortiClient console
  - Shutdown FortiClient
- Dynamic menu options depending on configuration
  - Connect to a configured IPsec VPN or SSL VPN connection
  - Display the antivirus scan window (if a scheduled scan is currently running)
  - Display the Vulnerability scan window (if a vulnerability scan is running)

If you hover the mouse cursor over the FortiTray icon, you will receive various notifications including the version, antivirus signature, and antivirus engine.

When the configuration is locked, the option to shut down FortiClient from FortiTray is greyed out.

Connect to a VPN connection

To connect to a VPN connection from FortiTray, select the Windows System Tray and right-click in the FortiTray icon. Select the connection you wish to connect to, enter your username and password in the authentication window, and select *OK* to connect.

Custom FortiClient Installations

The FortiClient Configurator tool FortiClient is the recommended method of creating customized FortiClient installation files.

	You can also customize which modules are displayed in the FortiClient dashboard in the FortiClient Profile. This will allow you to activate any of the modules at a later date without needing to re-install FortiClient. Any changes made to the FortiClient Profile are pushed to registered clients.
	When creating VPN only installation files, you cannot enable other modules in the FortiClient Profile as only the VPN module is installed.
	When deploying a custom FortiClient XML configuration, use the advanced FortiClient Profile options in FortiGate to ensure the FortiClient Profile settings do not overwrite your custom XML settings. For more information, see the *FortiClient XML Reference* and the *CLI Reference for FortiOS*.

The FortiClient Configurator tool is included with the FortiClient Tools file in FortiClient v5.2. This file is only available on the Customer Service & Support portal and is located in the same file directory as the FortiClient images.

The Configurator tool requires activation with a license file. Ensure that you have completed the following steps prior to logging in to your FortiCare product web portal:

- Purchased FortiClient Registration License
- Activated the FortiClient license on a FortiGate

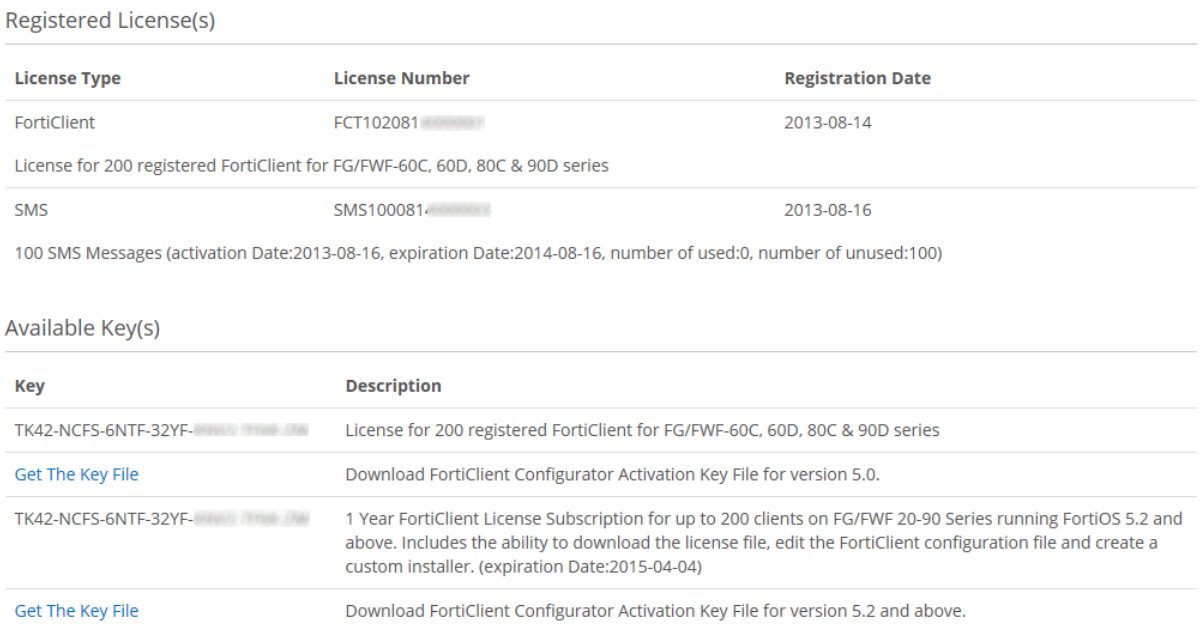
This video explains how to purchase and apply a FortiClient License:
http://www.youtube.com/watch?feature=player_embedded&v=sIkWaUXK0Ok

This chapter contains the following sections:

Download the license file

To retrieve your license file:

1. Go to https://support.fortinet.com and login to your FortiCare account.
2. Under *Asset* select *Manage/View Products*. Select the FortiGate device that has the FortiClient registration license activated. You will see the *Get the Key File* link in the *Available Key(s)* section.



Registered License(s)

License Type	License Number	Registration Date
FortiClient	FCT102081	2013-08-14
License for 200 registered FortiClient for FG/FWF-60C, 60D, 80C & 90D series		
SMS	SMS100081	2013-08-16
100 SMS Messages (activation Date:2013-08-16, expiration Date:2014-08-16, number of used:0, number of unused:100)		

Available Key(s)

Key	Description
TK42-NCFS-6NTF-32YF-	License for 200 registered FortiClient for FG/FWF-60C, 60D, 80C & 90D series
Get The Key File	Download FortiClient Configurator Activation Key File for version 5.0.
TK42-NCFS-6NTF-32YF-	1 Year FortiClient License Subscription for up to 200 clients on FG/FWF 20-90 Series running FortiOS 5.2 and above. Includes the ability to download the license file, edit the FortiClient configuration file and create a custom installer. (expiration Date:2015-04-04)
Get The Key File	Download FortiClient Configurator Activation Key File for version 5.2 and above.

3. Click the link and download license file to your management computer. This file will be needed each time you use the FortiClient Configurator tool.

FortiClient v5.2 cannot use FortiClient v5.0 licenses. To use FortiClient Configurator, you need to use the FortiClient v5.2 license file.

Create a custom installer

Fortinet offers a repacking tool for both Microsoft Windows and Mac OS X operating systems. The following section provides instructions on creating a custom installer file using the FortiClient Configurator tool.

When selecting to install custom features, only modules selected are installed. To enable other features you will need to uninstall FortiClient, and reinstall an MSI file with these features included in the installer.

FortiClient (Windows) Configurator tool

To create a custom installer using the FortiClient Configurator tool:

1. Unzip the FortiClientTools file, select the FortiClientConfigurator file folder, and double-click the *FortiClientConfigurator.exe* application file to launch the tool. The tool opens at the *Welcome* page.

Licensed	Licensed mode requires a FortiClient v5.2 license file.

Trial	In FortiClient v5.2, the FortiClient Configurator tool can be used in trial mode. In trial mode, all online updates are disabled. The trial installer is intended to be deployed in a test environment.

2. Browse and select the FortiClient Configurator Activation Key file (`.lic`) on your management computer.

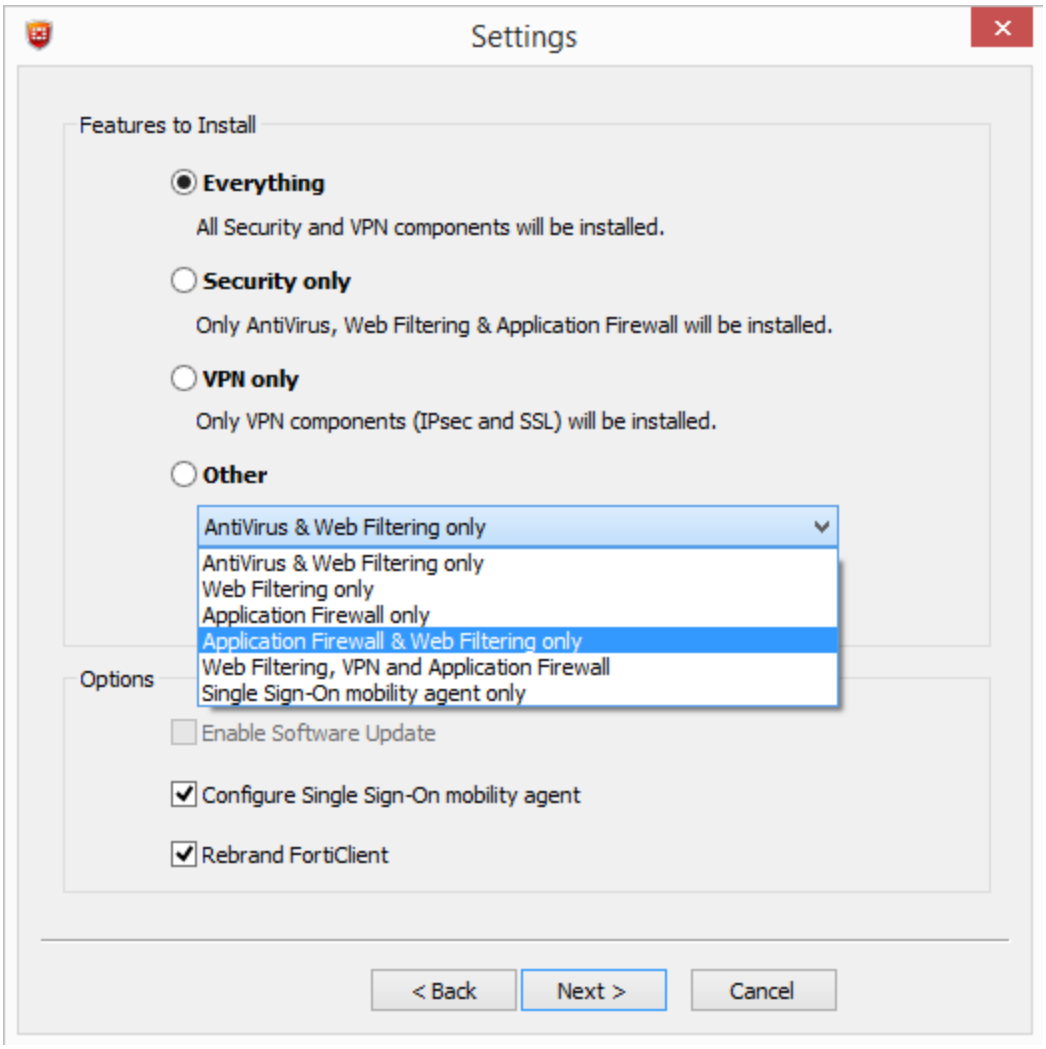
The FortiClient Configurator tool is not installed on the management computer. You must upload the FortiClient Configurator Activation Key file (`.lic`) each time you run the tool.

3. After entering the FortiClient Configurator license, select *Next*. The *Configuration File* page is displayed.

Select Config File (optional)	The configuration file (`.conf`, `.sconf`) settings will be included in the installer file.
Password	If the configuration file is encrypted (`.sconf`), enter the password used to encrypt the file.

You can use an XML editor to make changes to the FortiClient configuration file. For more information on FortiClient XML configuration, see the *FortiClient XML Reference* in the Fortinet Document Library, http://docs.fortinet.com.

4. Browse and select the FortiClient configuration file on your management computer. This is an optional step. If you do not want to import settings from a configuration file, select *Skip* to continue. The *Settings* page is displayed.

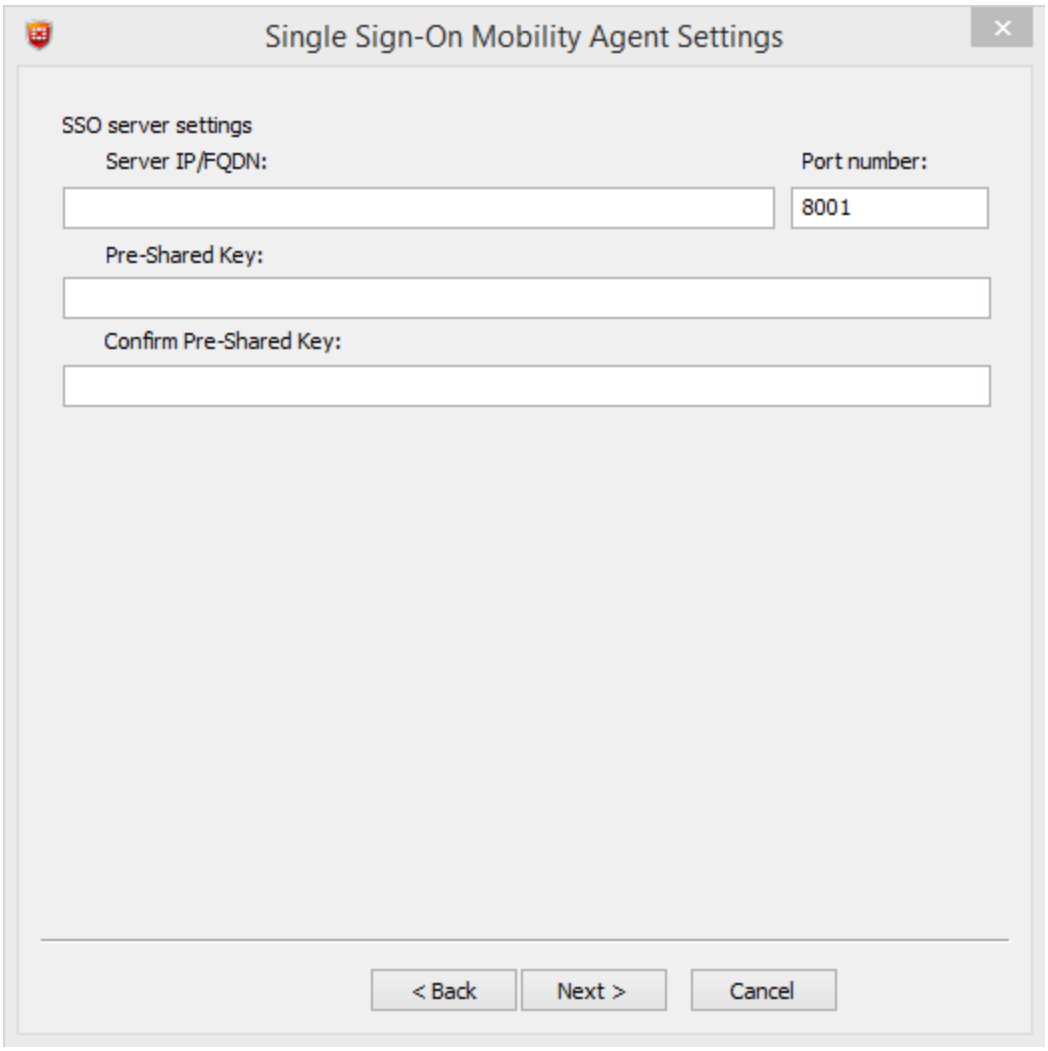


The following options are available for custom installations:

Features to Install	
Everything	All Security and VPN components will be installed.
Client security only	Only AntiVirus, Web Filtering, and Application Firewall will be installed.
VPN only	Only VPN components (IPsec and SSL) will be installed.

	Other	Select one of the following from the drop-down list: • AntiVirus & Web Filtering only • Web Filtering only • Application Firewall only • Application Firewall & Web Filtering only • Web Filtering, VPN and Application Firewall • Single Sign-On mobility agent only
Options		
	Desktop Shortcut	Select to create a FortiClient desktop icon.
	Start Menu	Select to add FortiClient to the start menu.
	Enable Software Update	Select to enable software updates. This option is disabled when *Rebrand FortiClient* is selected. This option is also disabled when using Trial mode.
	Configure Single Sign-On mobility agent	Select to configure Singe Sign-On mobility agent for use with FortiAuthenticator.
	Rebrand FortiClient	Select to rebrand FortiClient. When selected, the option to enable software update is not available. For more information on rebranding FortiClient, see Appendix C - Rebranding FortiClient on page 172.

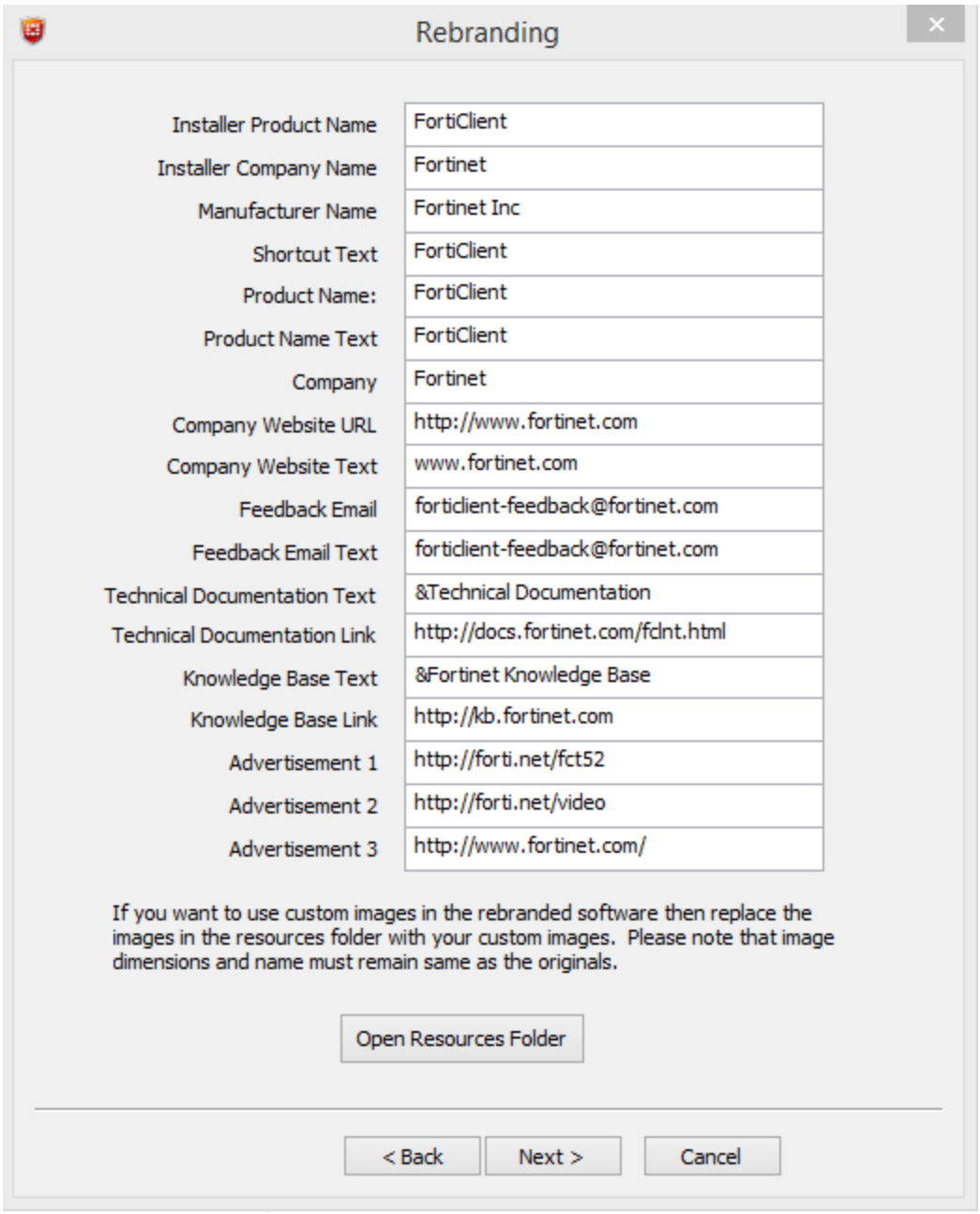
5. Select the features to install and options and select *Next* to continue.
   If you selected to configure the single sign-on mobility agent, the *Single Sign-On Mobility Agent Settings* page is displayed.



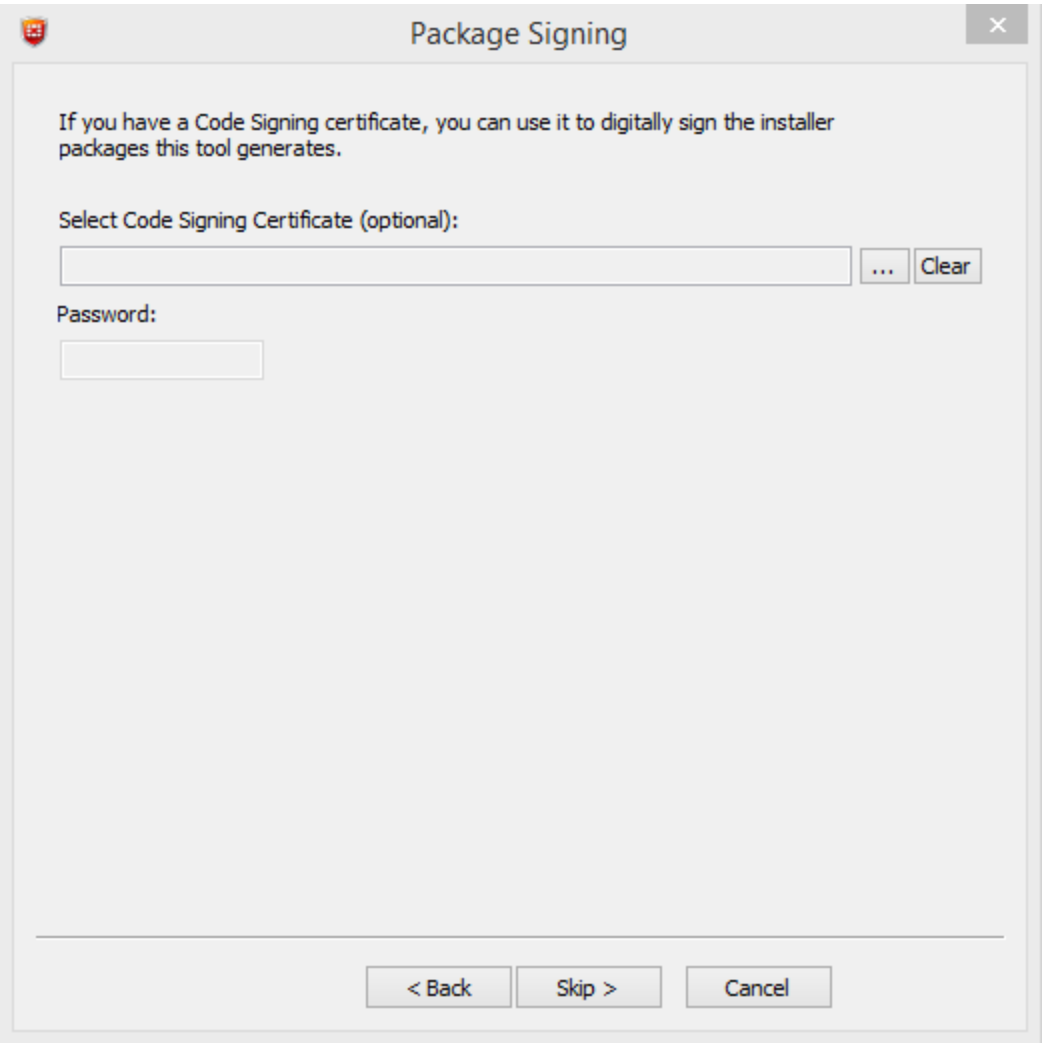
6. Configure the following settings:

Server IP/FQDN	Enter the IP address or FQDN of the FortiAuthenticator server.
Port Number	Enter the port number. The default port is 8001.
Pre-Shared Key	Enter the FortiAuthenticator pre-shared key.
Confirm Pre-Shared Key	Enter the FortiAuthenticator pre-shared key confirmation.

7. Select *Next* to continue. If you selected to rebrand FortiClient, the *Rebranding* page is displayed.



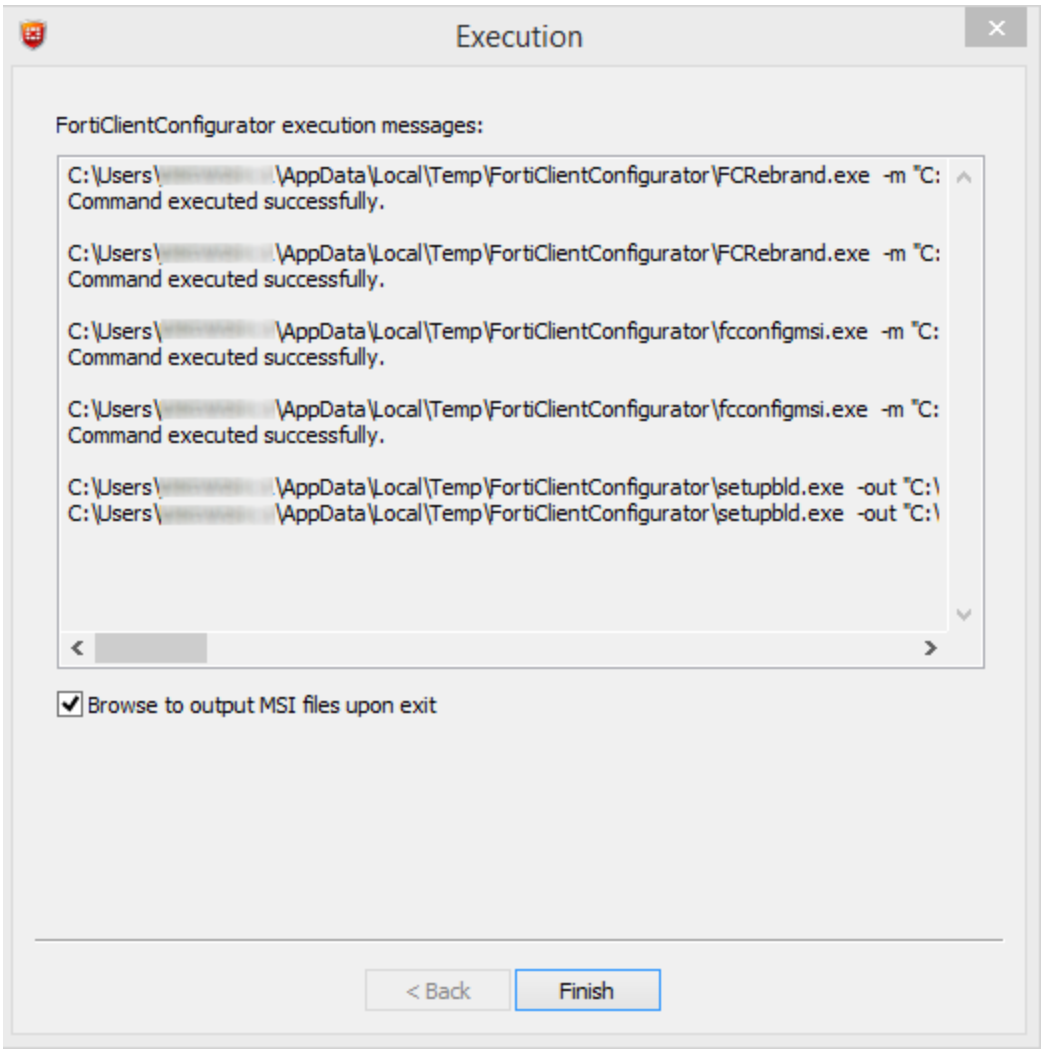
8. Rebrand FortiClient elements as required. The resources folder contains graphical elements. For more information on rebranding FortiClient, see Appendix C - Rebranding FortiClient on page 172.
9. Select *Next* to continue. The *Package Signing* page is displayed.



10. Configure the following settings:

Select Code Signing Certificate (optional)	If you have a code signing certificate, you can use it to digitally sign the installer package this tool generates.
Password	If the certificate file is password protected, enter the password.

11. Browse and select the code signing certificate on your management computer. This is an optional step. If you do not want to digitally sign the installer package, select *Skip* to continue. The *Execution* page is displayed.



This page provides details of the installer file creation and the location of files for Active Directory deployment and manual distribution. The tool creates files for both 32-bit (x86) and 64-bit (x64) operating systems.

12. When you select *Finish*, if *Browse to output MSI file upon exit* is selected, the folder containing the newly created MSI file will open.

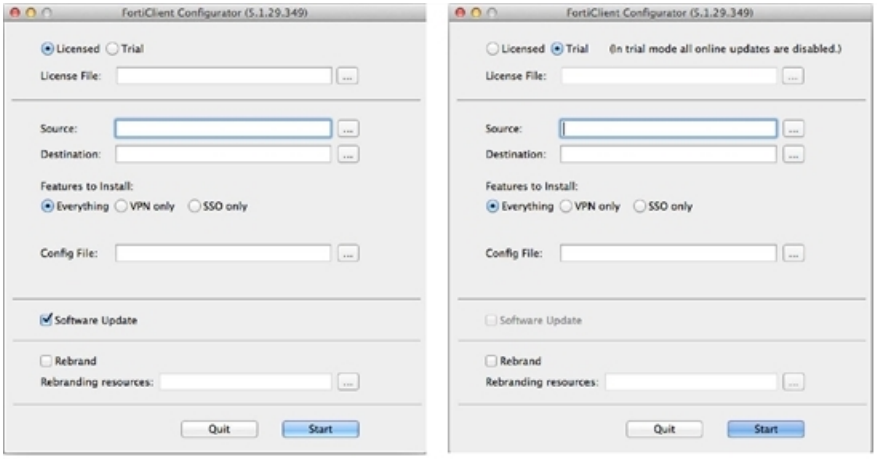
	Before deploying the custom MSI files, it is recommended that you test the packages to confirm that they install correctly. In FortiClient v5.2.0 and later, an `.exe` installation file is created for manual distribution.

	Installation files are organized in folders within the *FortiClientTools > FortiClient Configurator > FortiClient repackaged* folder. Folder names identify the type of installation files that were created and the creation date.

FortiClient (Mac OS X) Configurator tool

To create a custom installer using the FortiClient Configurator tool:

1. Unzip the FortiClientTools file, select the Configurator file folder, and double-click the *FortiClientConfigurator.dmg* application file, and double-click the FCTConfigurator icon to launch the tool. The *Configurator* tool opens.

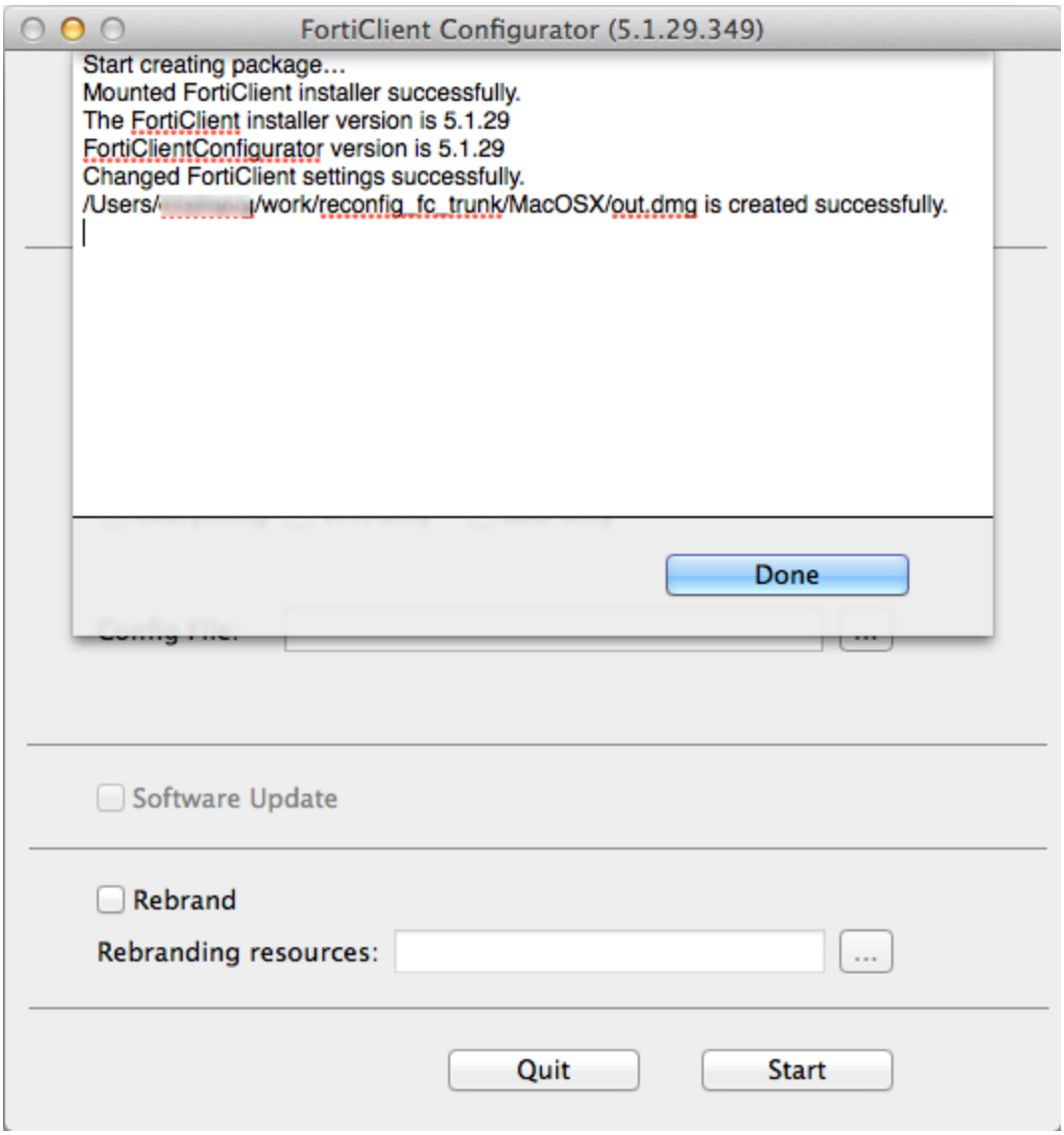


2. Configure the following settings:

Licensed | Trial	Licensed mode requires a FortiClient v5.2 license file. In FortiClient v5.2, the FortiClient Configurator tool can be used in trial mode. In trial mode, all online updates are disabled. The trial installer is intended to be deployed in a test environment.
Source	Select the FortiClient Installer file on your management computer. You must use the full installer file, otherwise FortiClient Configurator will fail to create a custom installation file. The FortiClient Installer version and FortiClient Configurator version must match, otherwise the Configurator will fail to create a custom installation file.
Destination	Enter a name for the custom installation file and select a destination to save the file on your management computer.
Features to Install	Select to install all FortiClient modules, VPN only, or SSO only. If SSO only is selected, you must configure the SSO settings in the attached configuration file.
Server IP/FQDN	Enter the IP address or FQDN of the FortiAuthenticator server. This option is available when selecting SSO only for features to install.
Port Number	Enter the port number. The default port is 8001. This option is available when selecting SSO only for features to install.

Pre-Shared Key	Enter the FortiAuthenticator pre-shared key. This option is available when selecting SSO only for features to install.
Confirm Pre-Shared Key	Enter the FortiAuthenticator pre-shared key confirmation. This option is available when selecting SSO only for features to install.
Config file	Optionally, select a pre-configured FortiClient backup configuration file. If you selected *Everything* or *VPN only* for features to install, you must use a configuration file to configure the related settings.
Software Update	Select to enable or disable software updates.
Rebrand	Select to rebrand FortiClient. When selected, the option to enable software update is not available. For more information on rebranding FortiClient, see Appendix C - Rebranding FortiClient on page 172.
Rebranding resources	Select the FortiClient resources file on your management computer.

3. Select the *Start* button to create the custom FortiClient installation file.



You can now deploy the repackaged FortiClient `.dmg` file to your Mac OS X systems.

Custom installation packages

When deploying a custom FortiClient XML configuration, use the advanced FortiClient Profile options in FortiGate to ensure the FortiClient Profile settings do not overwrite your custom XML settings. For more information, see the *FortiClient XML Reference* and the *CLI Reference for FortiOS*.

FortiClient (Windows)

After the configurator tool generates the custom installation packages, it can be used to deploy the FortiClient software either manually, or using Active Directory. Both options can be found in the *.../FortiClient_packaged*

directory. Files are created for both x86 (32-bit) and x64 (64-bit) operating systems.

If Active Directory is being used to deploy FortiClient, you can use the custom installer with the MST file found in the *.../ActiveDirectory* folder.

For manual distribution, use the `.exe` file in the *.../ManualDistribution* folder.

Advanced FortiClient profiles

When creating custom FortiClient MSI files for deployment, you will need to configure advanced FortiClient profiles on the FortiGate to ensure that settings in the FortiClient profile do not overwrite your custom XML settings. You can configure the FortiClient profile to deliver the full XML configuration, VPN only, or specific FortiClient XML configurations. For more information on customizing the FortiClient XML configuration file, see the FortiClient XML ReAppendix C - Rebranding FortiClientference.

Fortinet recommends creating OS specific endpoint profiles when provisioning XML settings. When creating a new FortiClient profile, select the device group as either Windows PC or Mac. If a FortiClient (Windows) XML configuration is pushed to a FortiClient (Mac OS X) system, FortiClient (Mac OS X) will ignore settings which are not supported.

Provision a full XML configuration file

You can deploy the full XML configuration file from the CLI or GUI.

To deploy the full XML configuration via the CLI:

1. Log in to the FortiGate Command-line Interface.
2. Enter the following CLI commands:

```
config endpoint-control profile
   edit <profile_name>
   config forticlient-winmac-settings
      set forticlient-advanced-cfg enable
      set forticlient-advanced-cfg-buffer "Copy & Paste your FortiClient XML
          configuration here"
   end
end
```

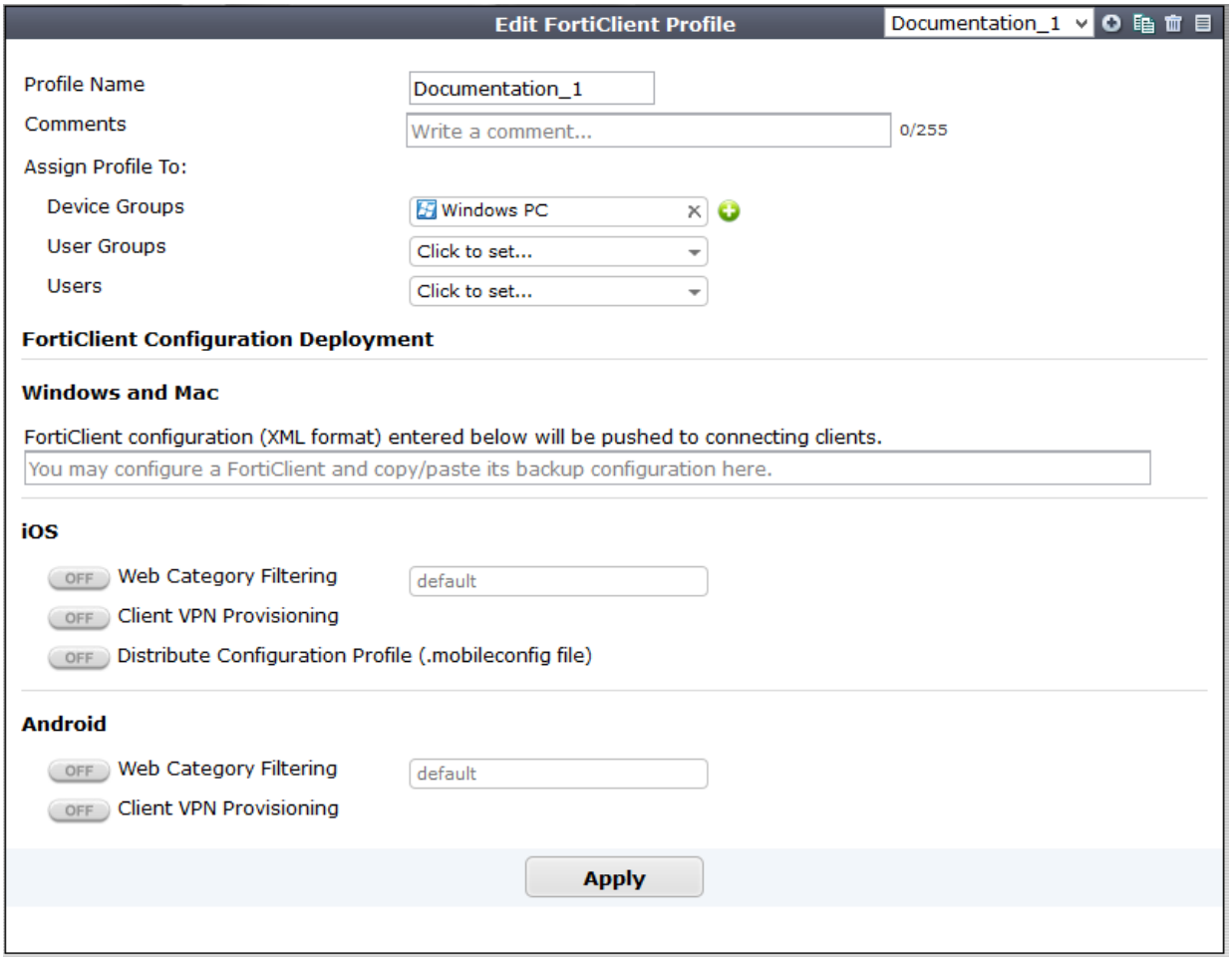
After `forticlient-advanced-cfg` is enabled, the `forticlient-advanced-cfg-buffer` CLI command is available from the CLI.

The buffer size for the FortiClient Control XML configuration is 32kB.

Copy directly from your XML editor, preserving the XML file format. Copy all information from the `<?xml version="1.0" encoding="UTF-8" ?>` start of syntax to the `</forticlient_configuration>` end of syntax XML tags. Add double quotes at the start and end of the XML syntax statements.

To deploy the full XML configuration via the GUI:

1. Go to *User & Device FortiClient Profiles*.
2. Select the FortiClient Profile and select *Edit* from the toolbar. The *Edit FortiClient Profile* page is displayed.



Configure the following settings:

Profile Name	Enter a unique name to identify the FortiClient profile.
Comments	Optionally, enter a comment.
Assign Profile To	For more information on configuring device groups, user groups, and users, see the *FortiOS Handbook*. These options are only available when creating a new FortiClient profile. You can assign the profile to user groups and users when using Active Directory authentication or RADIUS authentication for VPN. FortiClient does not support nested groups in FortiOS.
Device Groups	Select device groups from the drop down-menu. Use the add icon to add more than one device group.

	User Groups	Select user groups from the drop-down list. Use the add icon to add more than one device group.
	Users	Select users from the drop-down list. Use the add icon to add more than one device group.
FortiClient Configuration Deployment - Windows and Mac		
	XML text window	Cut and paste the FortiClient XML configuration file in the text window. The XML syntax must be preserved.

3. Select *Apply* to save the FortiClient profile settings.

The current buffer size is 32kB. This may not be large enough to accommodate your FortiClient XML configuration. As a workaround, you can use the FortiClient Configurator tool to create a custom MSI installation file using a `.conf` FortiClient backup configuration that contains static custom configurations. You can then include a partial configuration in the advanced FortiClient profile. This will push the partial configuration when the client registers with the FortiGate. The partial configuration will be merged with the existing XML configuration on the client.

To provision specific FortiClient XML configuration while preserving custom XML configurations in your MSI file, cut & paste the specific XML configuration into the FortiClient Profile in the following format:

```
<?xml version="1.0" encoding="UTF-8" ?>
<forticlient_configuration>
   <partial_configuration>1</partial_configuration>
   <system>
      <ui>
         <ads>0</ads>
         <default_tab>VPN</default_tab>
         <flashing_system_tray_icon>0</flashing_system_tray_icon>
         <hide_system_tray_icon>0</hide_system_tray_icon>
         <suppress_admin_prompt>0</suppress_admin_prompt>
         <culture_code>os-default</culture_code>
      </ui>
      <update>
         <use_custom_server>0</use_custom_server>
         <port>80</port>
         <timeout>60</timeout>
         <failoverport>8000</failoverport>
         <fail_over_to_fdn>1</fail_over_to_fdn>
         <scheduled_update>
            <enabled>0</enabled>
            <type>interval</type>
            <daily_at>03:00</daily_at>
            <update_interval_in_hours>3</update_interval_in_hours>
      </scheduled_update>
      </update>
   </system>
</forticlient_configuration>
```

Ensure that the `<partial_configuration>1</partial_configuration>` tag is set to 1 to indicate that this partial configuration will be deployed upon registration with the FortiGate. All other XML configuration will be preserved.

Advanced VPN provisioning

You need to enable VPN provisioning and advanced VPN from the FortiOS CLI to import the FortiClient XML VPN configuration syntax. You can import the XML VPN configuration in the CLI or the GUI.

Import XML VPN configuration into the FortiClient Profile via the CLI:

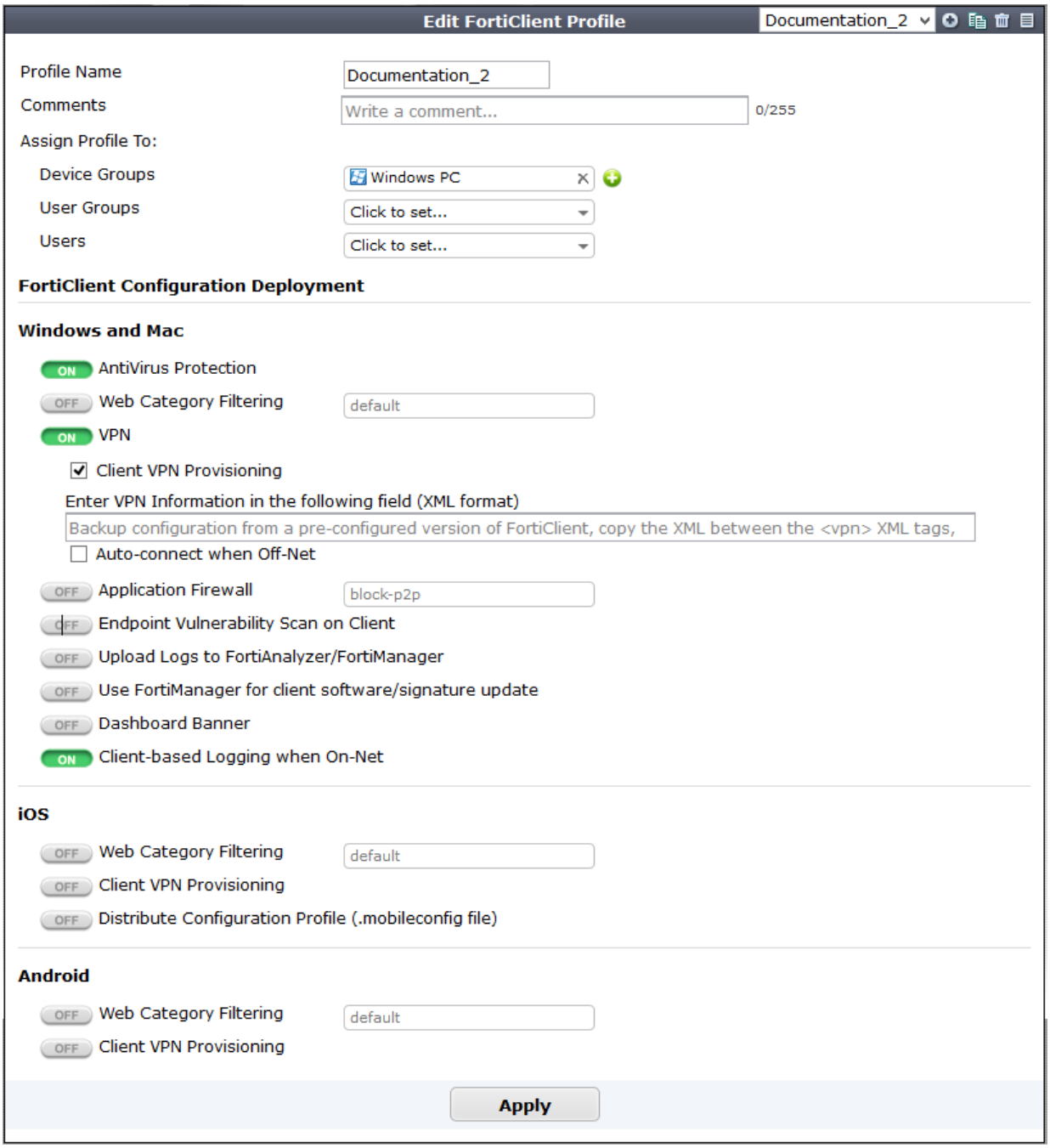
1. Log in to your FortiGate command-line interface.
2. Enter the following CLI commands:

```
config endpoint-control profile
   edit <profile_name>
   config forticlient-winmac-settings
      set forticlient-vpn-provisioning enable
      set forticlient-advanced-vpn enable
      set auto-vpn-when-off-net enable
      set auto-vpn-name <VPN name to connect to automatically when off-net>
      set forticlient-advanced-vpn-buffer <Copy & paste the advanced VPN
          configuration>
   end
end
```

After the `forticlient-vpn-provisioning` and `forticlient-advanced-vpn` CLI commands are enabled, the `forticlient-advanced-vpn-buffer` CLI command is available from the CLI.

Copy directly from your XML editor, preserving the XML file format. Copy all information from the `<vpn>` start of syntax to the `</vpn>` end of syntax XML tags. Add double quotes before the <vpn> tag and after the </vpn> tag.

3. You can also choose to copy & paste the XML content in the GUI, go to *User & Device* > *FortiClient Profiles*.



4. Configure the following settings:

Profile Name	Enter a unique name to identify the FortiClient profile.
Comments	Optionally, enter a comment.

Assign Profile To	For more information on configuring device groups, user groups, and users, see the *FortiOS Handbook*. These options are only available when creating a new endpoint profile. You can assign the profile to user groups and users when using Active Directory authentication or RADIUS authentication for VPN. FortiClient does not support nested groups in FortiOS.
Device Groups	Select device groups from the drop down-menu. Use the add icon to add more than one device group.
User Groups	Select user groups from the drop-down list. Use the add icon to add more than one device group.
Users	Select users from the drop-down list. Use the add icon to add more than one device group.
FortiClient Configuration Deployment Windows and Mac	
AntiVirus Protection	Toggle the button on or off to enable or disable this feature.
Web Category Filtering	Toggle the button on or off to enable or disable this feature. When enabled, you can select a web filter profile in the drop-down list. Select the checkbox to enable client web filtering when on-net.
VPN	Select the checkbox for Client VPN Provisioning. Cut and paste the FortiClient XML configuration `<vpn>` to `</vpn>` tags in the text window. The XML syntax must be preserved. Select the checkbox to enable auto-connect when off-net and select a VPN connection in the drop-down list.
Application Firewall	Toggle the button on or off to enable or disable this feature. When enabled, you can select an application control sensor in the drop-down list.
Endpoint Vulnerability Scan on Client	Toggle the button on or off to enable or disable this feature. When enabled, you can select the scheduled scan type to daily, weekly, or monthly. Select the checkbox to initiate a scan after client registration with the FortiGate. This feature must be enabled per FortiClient profile in the FortiOS CLI.
Upload Logs to FortiAnalyzer/FortiManager	Toggle the button on or off to enable or disable this feature. When enabled, you can select to use the same FortiAnalyzer/FortiManager used by the FortiGate or select Specify to enter a different device IP. You can set the schedule to hourly or daily. The FortiClient upload logs to the FortiAnalyzer/FortiManager only when it is able to connect to the device on the specified IP address.
Use FortiManager for client software/signature update	Toggle the button on or off to enable or disable this feature. When enabled, you can specify the IP address of the FortiManager. Select the checkbox to failover to the FortiGuard Distribution Network (FDN) when the FortiManager is not available.

Dashboard Banner	Toggle the button on or off to enable or disable this feature.
Client-based Logging when On-Net	Toggle the button on or off to enable client-based logging when on-net.

5. Select *Apply* to save the FortiClient profile settings.
   For more information, see Appendix A - Deployment Scenarios on page 158.

Upgrade Information

FortiClient (Windows) 5.2.6 upgrade information

Please review the *FortiClient (Windows) 5.2.6 Release Notes* prior to upgrading your client. The following information outlines supported upgrade paths and methods.

When upgrading on a Windows XP system, a warning dialog box is displayed indicating that one of the files to be updated is currently in use. Please select the `Ignore` button to continue with the upgrade.
Users with newer Windows OS versions will receive a different warning dialog box. It warns that a reboot will be required to complete the installation. Please click the *OK* button to continue with the installation.

FortiClient (Mac OS X) 5.2.6 upgrade information

Please review the *FortiClient (Mac OS X) 5.2.6 Release Notes* prior to upgrading your client. The following information outlines supported upgrade paths and methods.

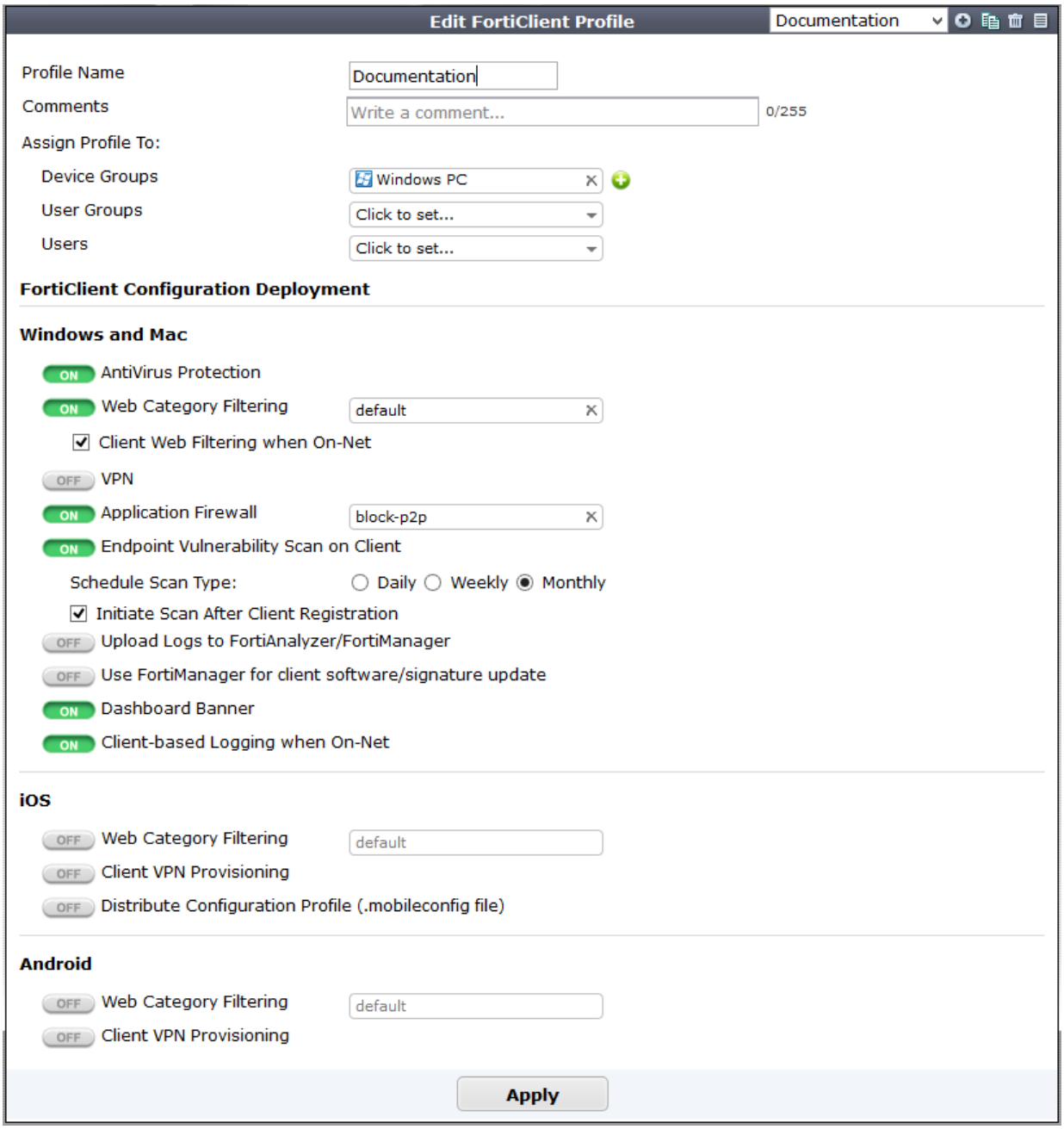
Appendix A - Deployment Scenarios

Basic FortiClient Profile

In this scenario, you want to configure all FortiClient Profile settings in the FortiGate GUI. When clients register, they will receive the settings configured in the FortiClient Profile. You can configure the default profile, or create a new profile. When creating a new profile, you have additional options to specify device groups, user groups, and users.

Create a basic FortiClient Profile:

1. In the FortiGate GUI, go to *User & Device* > *FortiClient Profiles*. You can either select the default FortiClient Profile or select *Create New* in the toolbar. The default FortiClient Profile does not include the *Device Groups, User Groups,* and *Users* settings. The *Edit Endpoint Profile* page opens.



2. Set the device groups, user groups, user settings, and other FortiClient Profile settings as required and select *Apply* to save the FortiClient Profile changes.

Advanced FortiClient Profile (Full XML Configuration)

In this scenario, you have created a custom XML configuration file. The custom file includes all settings required by the client at the time of deployment. When the client registers to the FortiGate, you want to ensure that the client receives the full XML configuration. For future configuration changes you can use the Advanced FortiClient Profile (Partial XML Configuration) on page 161 procedure.

The buffer size in the FortiClient Profile is 32kB. Depending on the size of the FortiClient XML configuration file you may not be able to deploy the full XML configuration file in the FortiClient Profile. Alternatively, you can create a custom installation file with the repackager tool and push a partial XML configuration. For more information, see Advanced FortiClient Profile (Partial XML Configuration) on page 161.

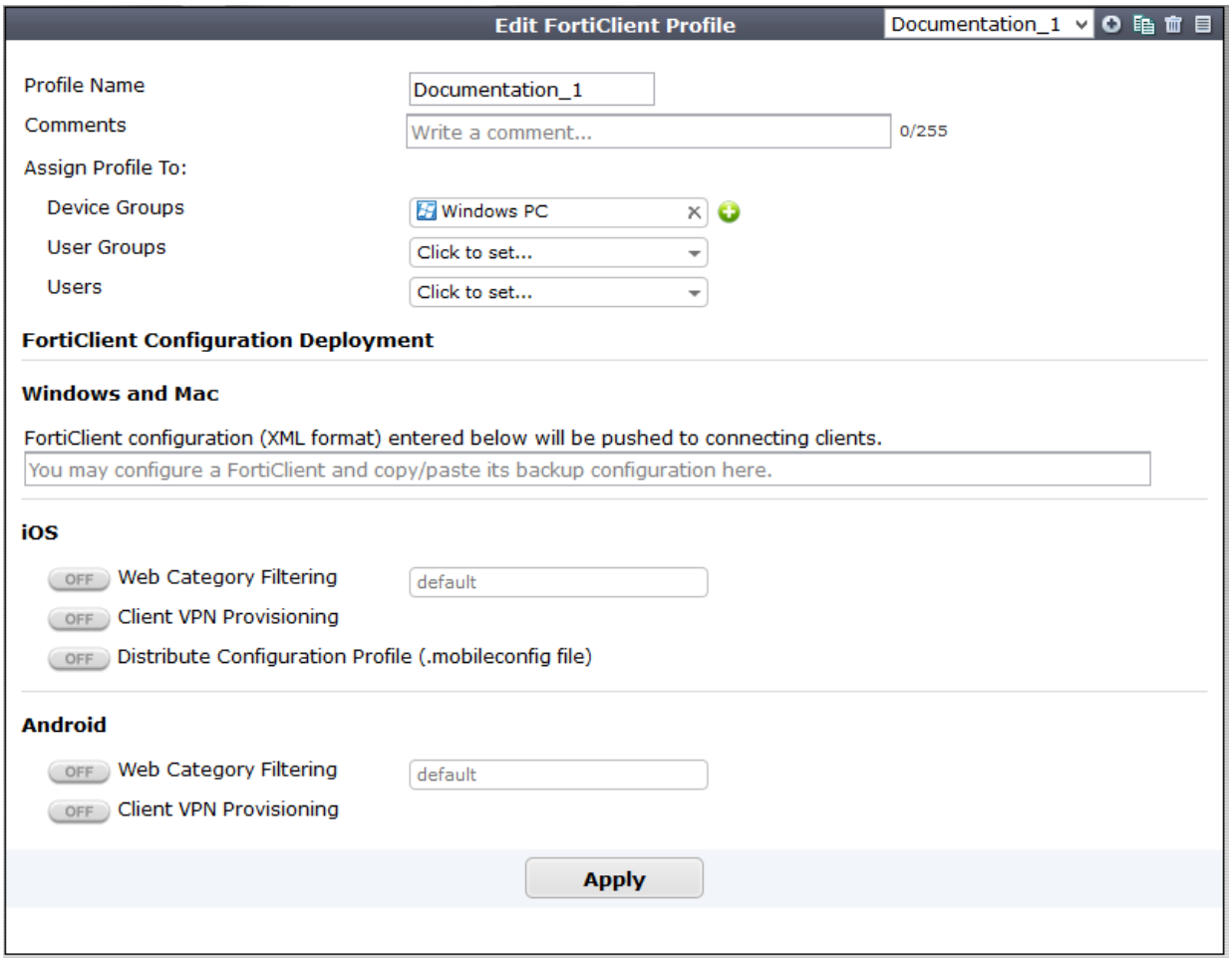
To reduce the size of the FortiClient XML configuration file, you can delete all help text found within the `<!-- .... -->` comment tags.

Create an advanced FortiClient Profile with the full XML configuration provisioned:

1. In the FortiGate Command-line Interface enter the following commands:

```
config endpoint-control profile
   edit <profile_name>
   config forticlient-winmac-settings
      set forticlient-advanced-cfg enable
   end
end
```

2. In the FortiGate GUI, go to *User & Device* > *FortiClient Profiles*. Select the advanced FortiClient profile and select *Edit* in the toolbar. The *Edit FortiClient Profile* page opens.



3. Open the FortiClient XML configuration file in a source code editor. Copy and paste the FortiClient XML configuration file into the XML text field in the FortiClient Profile.

Alternatively, you can copy and paste the XML configuration into the CLI using the `set forticlient-advanced-cfg-buffer` command.

4. Set the device groups, user groups, and user settings as required, and select *Apply* to save the FortiClient Profile changes. In the future, if you need to update the FortiClient configuration follow the procedure in Advanced FortiClient Profile (Partial XML Configuration) on page 161.

Advanced FortiClient Profile (Partial XML Configuration)

In this scenario, you have created a custom XML configuration file and you have created a custom FortiClient installation file using the repackaging tool. The custom XML configuration file includes most settings required by the client at the time of deployment. Due to the 32kB buffer size limitation, you are not able to follow Advanced FortiClient Profile (Full XML Configuration) on page 159 procedure.

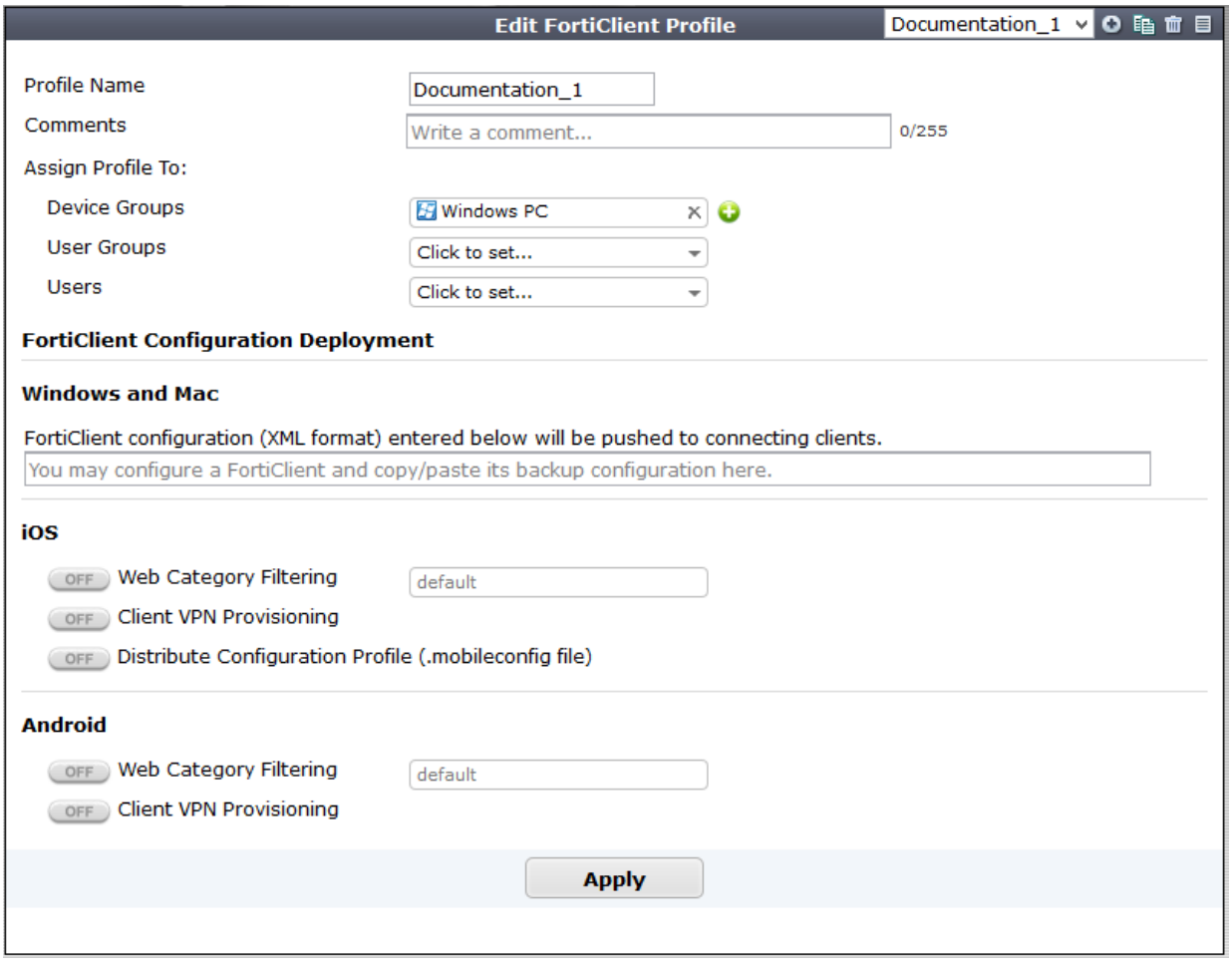
When the client registers to the FortiGate, you want to ensure that the client receives the partial XML configuration. The partial configuration will be merged with the existing XML configuration.

Create an advanced FortiClient Profile with the partial XML configuration provisioned:

1. In the FortiGate Command-line Interface enter the following commands:

```
config endpoint-control profile
   edit <profile_name>
   config forticlient-winmac-settings
      set forticlient-advanced-cfg enable
   end
end
```

2. In the FortiGate GUI, go to *User & Device* > *FortiClient Profiles*. Select the advanced FortiClient profile and select *Edit* in the toolbar. The *Edit FortiClient Profile* page opens.



3. Open the FortiClient XML configuration file in a source code editor. Copy and paste the following lines directly from the source code editor into the XML text field in the FortiClient profile:

```
<?xml version="1.0" encoding="UTF-8" ?>
<forticlient_configuration>
   <partial_configuration>1</partial_configuration>
   .......
</forticlient_configuration>
```

By setting the `<partial_configuration>` statement to `1`, the XML configuration will be merged into the existing XML configuration.

Alternatively, you can copy and paste the XML configuration into the CLI using the `set forticlient-advanced-cfg-buffer` command.

4. Set the device groups, user groups, and user settings as required and select *Apply* to save the FortiClient Profile changes. In the future if you need to update the FortiClient configuration follow the procedure in Advanced FortiClient Profile (Full XML Configuration) on page 159.

Advanced VPN Provisioning FortiClient Profile

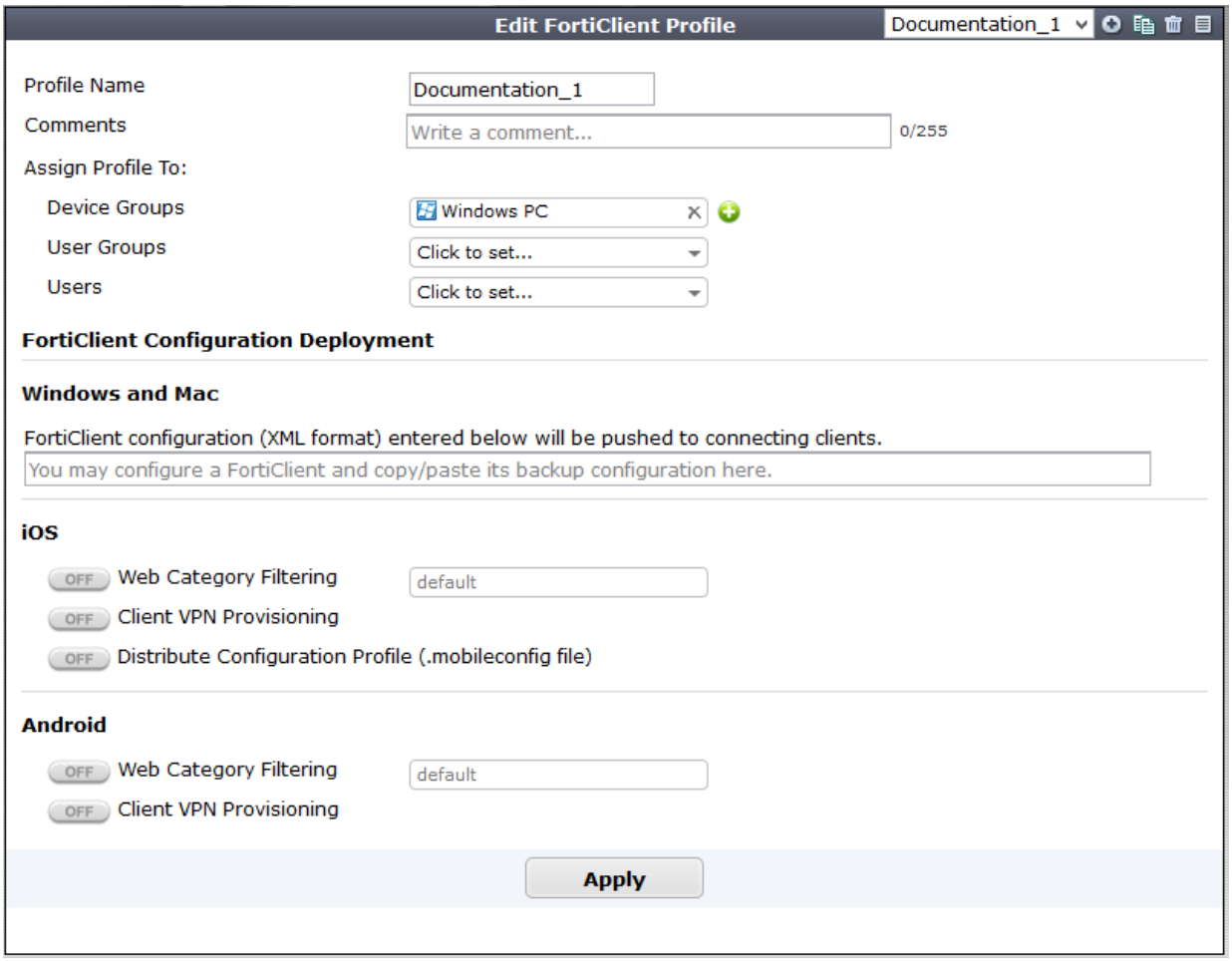
In this scenario, you want to provision multiple XML VPN configurations while setting the other FortiClient Profile settings in the FortiGate GUI. As the current buffer size in the CLI is 32kB, your FortiClient XML configuration may be too large to deploy using the regular advanced FortiClient Profile. You can use the repackaging tool to configure settings which are not available in the FortiClient Profile page by including the FortiClient XML configuration file in the installation

Create an advanced FortiClient Profile with XML VPN configurations:

1. In the FortiGate Command-line Interface enter the following commands:

```
config endpoint-control profile
   edit <profile_name>
   config forticlient-winmac-settings
      set forticlient-vpn-provisioning enable
      set forticlient-advanced-vpn enable
      set auto-vpn-when-off-net enable
      set auto-vpn-name <VPN name to connect to automatically when off-net>
   end
end
```

2. In the FortiGate GUI, go to *User & Device* > *FortiClient Profiles*. Select the advanced FortiClient profile and select *Edit* in the toolbar. The *Edit FortiClient Profile* page opens.



3. Open the FortiClient XML configuration file in a source code editor. Copy and paste all information from the `<vpn>` comment tag to the `</vpn>` comment tag directly from the source code editor into the XML text field in the endpoint profile.

Alternatively, you can copy and paste the XML configuration into the CLI using the `set forticlient-advanced-vpn-buffer` command.

4. Set the device groups, user groups, user settings, and other FortiClient Profile settings as required and select *Apply* to save the FortiClient Profile changes.

Advanced FortiClient Profile (No Settings Provisioned)

In this scenario, you have created a custom installation file using the repackager tool. The custom file includes all settings required by the client at the time of deployment. When the client registers to the FortiGate, you want to ensure that no settings are pushed to the client and the XML configuration remains intact.

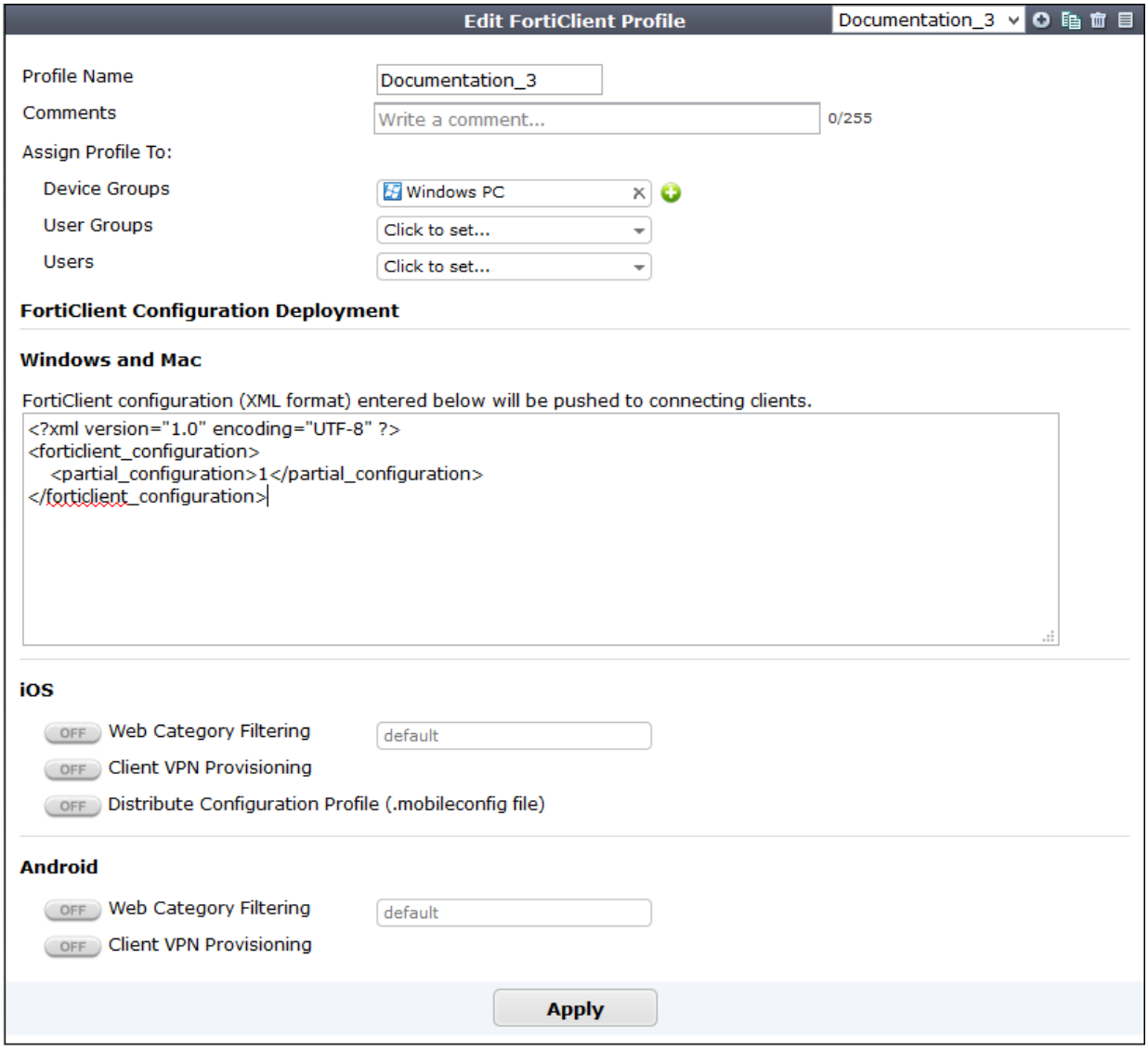
When changes are required you can push a partial configuration to the clients with the specific XML configuration changes.

Create an advanced FortiClient Profile with no settings provisioned:

1. In the FortiGate Command-line Interface enter the following commands:

```
config endpoint-control profile
   edit <profile_name>
   config forticlient-winmac-settings
      set forticlient-advanced-cfg enable
   end
end
```

2. In the FortiGate GUI, go to *User & Device* > *FortiClient Profiles*. Select the advanced FortiClient profile and select *Edit* in the toolbar. The *Edit FortiClient Profile* page opens.



3. Open the FortiClient XML configuration file in a source code editor. Copy and paste the following lines directly from the source code editor into the XML text field in the FortiClient profile:

```
<?xml version="1.0" encoding="UTF-8" ?>
<forticlient_configuration>
   <partial_configuration>1</partial_configuration>
</forticlient_configuration>
```

By setting the `<partial_configuration>` statement to `1`, the XML configuration will be merged into the existing XML configuration. Since no other XML statements are included, no changes will be made to the XML configuration on the client.

Alternatively, you can copy and paste the XML configuration into the CLI using the `set forticlient-advanced-cfg-buffer` command.

4. Set the device groups, user groups, and user settings as required and select *Apply* to save the FortiClient Profile changes. In the future if you need to update the FortiClient configuration follow the procedure in Advanced FortiClient Profile (Partial XML Configuration) on page 161.

Using Active Directory Groups

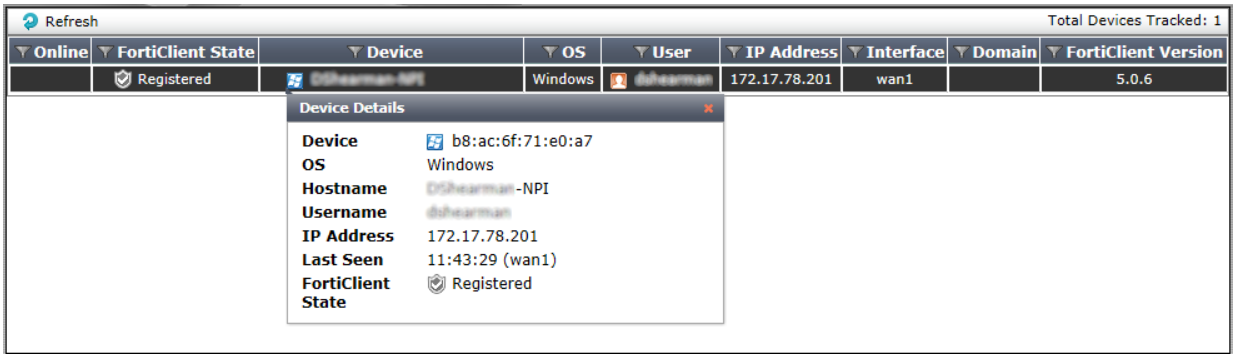
Some organisations may choose to deploy different FortiClient profiles to different user groups. FortiOS is able to send different FortiClient profiles based on the AD group of the user. This requires use of the FortiAuthenticator.

No special configuration is required on FortiClient.

Monitoring registered users

An administrator can monitor managed FortiClient users. When the client successfully registers to the FortiGate, the client can be monitored on the FortiGate.

In the FortiOS GUI, all registered clients can be observed on the *User & Device* > *Monitor* > *FortiClient* page.



Either of the following FortiOS CLI commands will list all registered clients:

- `diagnose endpoint registration list`, or
- `diagnose endpoint record-list`.

Customizing FortiClient using XML settings

FortiClient configurations can be customized at the XML level. For more information, see the *FortiClient XML Reference*.

Silent registration

You may want to configure FortiClient to silently register to FortiGate without any user interaction. When configured, the user will not be prompted to register to a FortiGate. The <silent_registration> tag is intended to be used with the <disable_unregister> tab. For more information, see Disable unregistration on page 167. The following XML elements can be used to enable this:

```
<forticlient_configuration>
   <endpoint_control>
      <silent_registration>1</silent_registration>
   </endpoint_control>
</forticlient_configuration>
```

Locked FortiClient settings

End-users with administrator permission on their Windows system have access to the FortiClient settings page. If this is not desired, it can be locked with a password from the FortiGate. The following FortiOS Command Line Interface (CLI) command, when included, requires that any client registered to the FortiGate to provide the password before they can access the settings page.

```
config endpoint-control profile
   edit "fmgr"
      config forticlient-winmac-settings
         ...
         set forticlient-settings-lock disable
         set forticlient-settings-lock-passwd <password>
         ...
         end
      ...
      next
   end
```

Disable unregistration

With silent endpoint control registration enabled, a user could unregister after FortiClient has registered to the FortiGate. The capability to unregister can be disabled using the following XML element:

```
<forticlient_configuration>
   <endpoint_control>
      <disable_unregister>1</disable_unregister>
   </endpoint_control>
</forticlient_configuration>
```

Putting it together

Here is a sample complete FortiClient 5.2.6 XML configuration file with the capabilities discussed above:

```
<forticlient_configuration>
   <partial_configuration>1</partial_configuration>
   <endpoint_control>
      <enabled>1</enabled>
      <disable_unregister>1</disable_unregister>
      <silent_registration>1</silent_registration>
      <fortigates>
         <fortigate>
```

```
            <serial_number />
            <name />
            <registration_password>un9r3Ak@b!e</registration_password>
            <addresses>newyork.example.com</addresses>
         </fortigate>
      </fortigates>
   </endpoint_control>
</forticlient_configuration>
```

The FortiGate that is registered to is listed in the `<fortigates>` element. The `<registration_password>` element is required if the endpoint control configuration on the FortiOS requires one. This can be exported as an encrypted file from a registered FortiClient.

The configuration provided above is not the full FortiClient configuration file. Thus, the `<partial_configuration>` element is set to `1`.

Off-net VPN auto-connect

Configure off-net VPN auto-connect and disable the VPN disconnect button

1. Configure the corresponding FortiClient profile from the FortiGate CLI. Enter the following CLI commands:

```
config endpoint-control profile
   edit <profile_name>
   config forticlient-winmac-settings
      set forticlient-vpn-provisioning enable
      set forticlient-advanced-vpn enable
end
```

2. Log into FortiGate GUI.
3. Go to *User & Device* > *FortiClient Profiles* and select the profile you edited in the previous step.
4. Copy and paste the VPN configuration in XML format into the VPN field. This includes the VPN connection and the settings for off-net VPN auto connect.

```
<vpn>
   <options>
      <autoconnect_tunnel>ssl209.77</autoconnect_tunnel>
      <autoconnect_only_when_offnet>1</autoconnect_only_when_offnet>
      <keep_running_max_tries>0</keep_running_max_tries>
      <allow_personal_vpns>0</allow_personal_vpns>
      <disable_connect_disconnect>1</disable_connect_disconnect>
   </options>
   <sslvpn>
      <options>
         <enabled>1</enabled>
      </options>
      <connections>
         <connection>
            <name>ssl209.77</name>
            <server>209.207.125.77:443</server>
            <username />
            <single_user_mode>0</single_user_mode>
            <ui>
               <show_remember_password>1</show_remember_password>
               <show_alwaysup>1</show_alwaysup>
               <show_autoconnect>1</show_autoconnect>
```

```
                </ui>
                <password />
                <certificate />
                <prompt_certificate>0</prompt_certificate>
                <prompt_username>1</prompt_username>
                <fgt>1</fgt>
                <on_connect>
                   <script>
                      <os>windows</os>
                      <script>
                      <![CDATA[]]>
                      </script>
                   </script>
                </on_connect>
                <on_disconnect>
                   <script>
                      <os>windows</os>
                      <script>
                      <![CDATA[]]>
                   </script>
                   </script>
                </on_disconnect>
             </connection>
          </connections>
       </sslvpn>
    </vpn>
```

5. FortiClient will receive the profile from the FortiGate upon registration. The user will be prompted to enter their username and password and connect to the VPN.
6. When FortiClient is detected as off-net, the VPN connection window will be displayed. The user will enter their username and password and connect to the VPN.
7. After the VPN is connected, the disconnect button will be disabled.
8. FortiClient will then always attempt to connect to the VPN.

Appendix B - Using the FortiClient API

You can operate FortiClient VPNs using the COM-based FortiClient API. The API can be used with IPsec VPN only. SSL VPN is currently not supported.

This chapter contains the following sections:

Overview

The FortiClient COM library provides functionality to:

- Retrieve a list of the VPN tunnels configured in the FortiClient application.
- Start and stop any of the configured VPN tunnels.
- Send XAuth credentials.
- Retrieve status information:
  - configured tunnel list
  - active tunnel name
  - connected or not
  - idle or not
  - remaining key life
- Respond to FortiClient-related events:
  - VPN connect
  - VPN disconnect
  - VPN is idle
  - XAuth authentication requested

For more information, see the vpn_com_examples ZIP file located in the VPN Automation file folder in the FortiClientTools file.

API reference

The following tables provide API reference values.

`Disconnect(bstrTunnelName As String)`	Close the named VPN tunnel.
`GetPolicy pbAV As Boolean, pbAS As Boolean, pbFW As Boolean, pbWF As Boolean)`	Command is deprecated in FortiClient v5.0.

`GetRemainingKeyLife(bstrTunnelName As String, pSecs As Long, pKBytes As Long)`	Retrieve the remaining key life for the named connection. Whether keylife time (pSecs) or data (pKBytes) are significant depends on the detailed settings in the FortiClient application.
`MakeSystemPolicyCompliant()`	Command is deprecated in FortiClient v5.0.
`SendXAuthResponse (tunnelName As String, userName As String, password As String, savePassword As Boolean)`	Send XAuth credentials for the named connection: • User name, Password • True if password should be saved.
`SetPolicy (bAV As Boolean, bAS As Boolean, bFW As Boolean, bWF As Boolean)`	Command is deprecated in FortiClient v5.0.

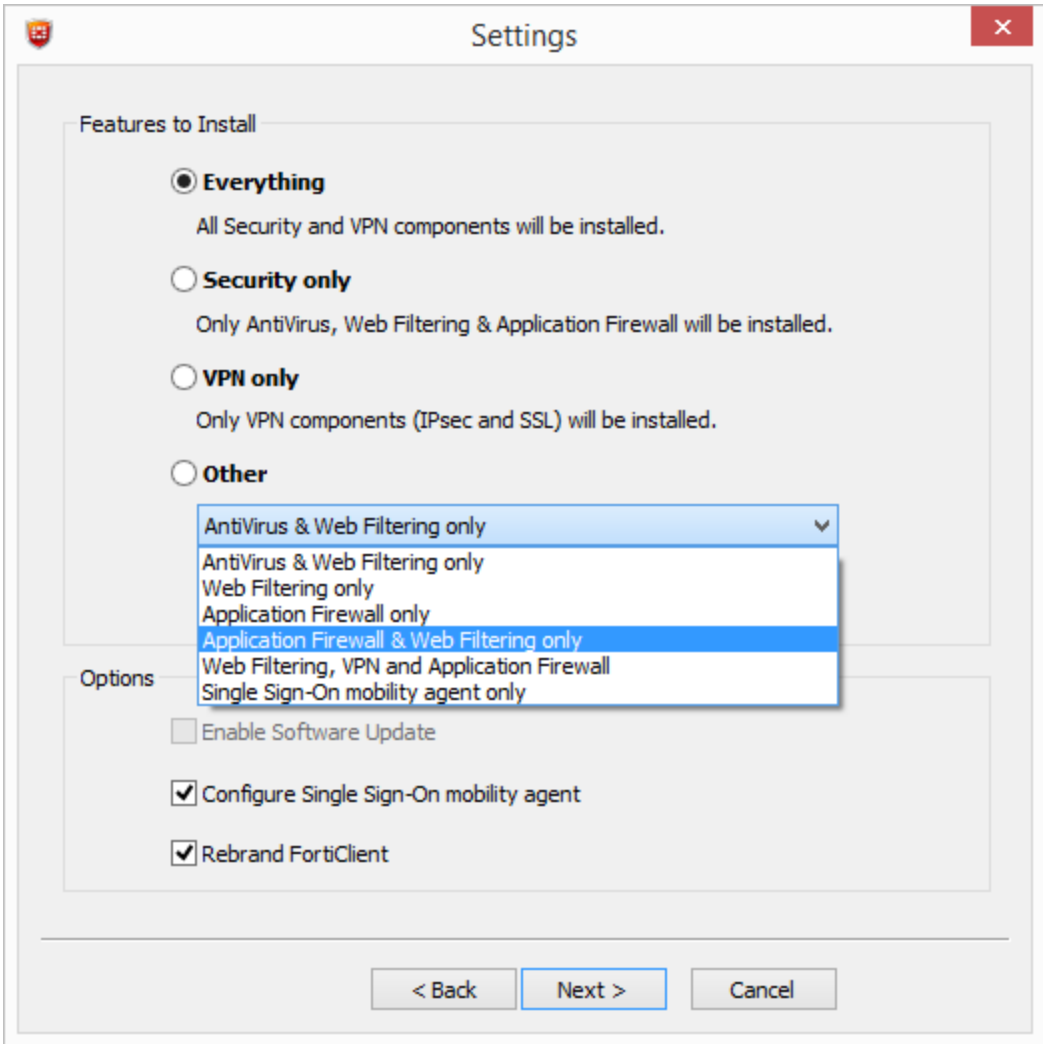
`GetTunnelList()`	Retrieve the list of all connections configured in the FortiClient application.
`IsConnected (bstrTunnelName As String) As Boolean`	Return True if the named connection is up.
`IsIdle (bstrTunnelName As String) As Boolean`	Return True if the named connection is idle.

`OnDisconnect(bstrTunnelName As String)`	Connection disconnected.
`OnIdle(bstrTunnelName As String)`	Connection idle.
`OnOutOfCompliance(bAV As Boolean, bAS As Boolean, bFW As Boolean, bWF As Boolean)`	Command is deprecated in FortiClient v5.0.
`OnXAuthRequest(bstrTunnelName As String)`	The VPN peer on the named connection requests XAuth authentication.

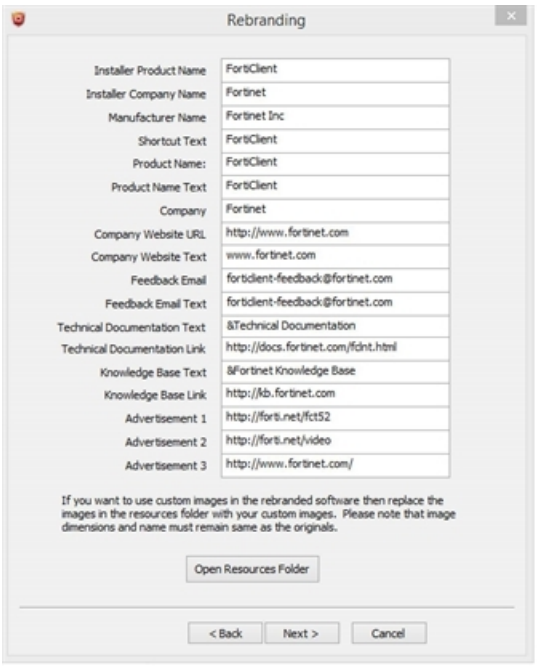
Appendix C - Rebranding FortiClient

The FortiClient Configurator can be used to create custom FortiClient MSI installers with various combinations. The customized MSI installer generated may be used to install FortiClient on all supported platforms using Active Directory or SCCM. A FortiClient setup executable file is also generated for manual distribution.

The FortiClient license for FortiOS 5.2 includes the license file required to use the FortiClient Configurator tool used to create custom FortiClient installers. The Configurator tool also allows you to rebrand the installer file.



Under *Options*, you can select to enable software updates, configure the single sign-on mobility agent, and rebrand FortiClient. Rebranding allows you to edit various UI elements including graphics.



When replacing files in the resource folder, the replacement file should be the same file type and dimensions. Icons (`.ico`) are a special case. The `Main_icon.ico` file for example, is a composite file of multiple icons. The operating system picks the appropriate icon size from this file for the context in which the icon is being displayed.

Rebranding elements:

Installer Product Name	Where Used: Setup Wizard header and body, File directory name in Installer Company Name file folder, engine/signature update bubble messages. Default Value: FortiClient
Installer Company Name	Where Used: File directory name in Program Files. Default Value: Fortinet
Manufacturer Name	Where Used: Default Value: Fortinet Inc
Shortcut Text	Where Used: Name of shortcut on desktop Default Value: FortiClient
Product Name	Where Used: Name of installer file (.msi/.mst), UI header, configuration received from FortiGate bubble messages, Default Value: FortiClient
Product Name Text	Where Used: Name of client in main page Default Value: FortiClient

Company	Where Used: *Help* > *About* > *Copyright* page Default Value: Fortinet
Company WebSite URL	Where Used: *Help* > *About* > *Copyright* page Default Value: http://www.fortinet.com
Company Website Text	Where Used: *Help* > *About* > *Copyright* page Default Value: www.fortinet.com
Feedback Email	Where Used: *Help* > *About* > *Copyright* page, Send Feedback Default Value: forticlient-feedback@fortinet.com
Feedback Email Text	Where Used: *Help* > *About* > *Copyright* page, Send Feedback Default Value: forticlient-feedback@fortinet.com
EULA	Where Used: *Help* > *About* > *Copyright* page, Click here to view the license agreement Default Value: http://www.fortinet.com/doc/legal/EULA.pdf
Knowledge Base Text	Where Used: Help menu option Default Value: Fortinet Knowledge Base Leave this field blank to omit the field in the console.
Knowledge Base Link	Where used: Link used by Knowledge Base text Default value: http://kb.fortinet.com Leave this field blank to omit the field in the console.
Advertisement 1	Where used: Link used by dashboard banner advertisement 1 Default value: http://www.forticlient.com/video/001
Advertisement 2	Where used: Link used by dashboard banner advertisement 2 Default value: http://www.forticlient.com/video/002
Advertisement 3	Where used: Link used by dashboard banner advertisement 3 Default value: http://www.forticlient.com/video/003

Resources folder elements:

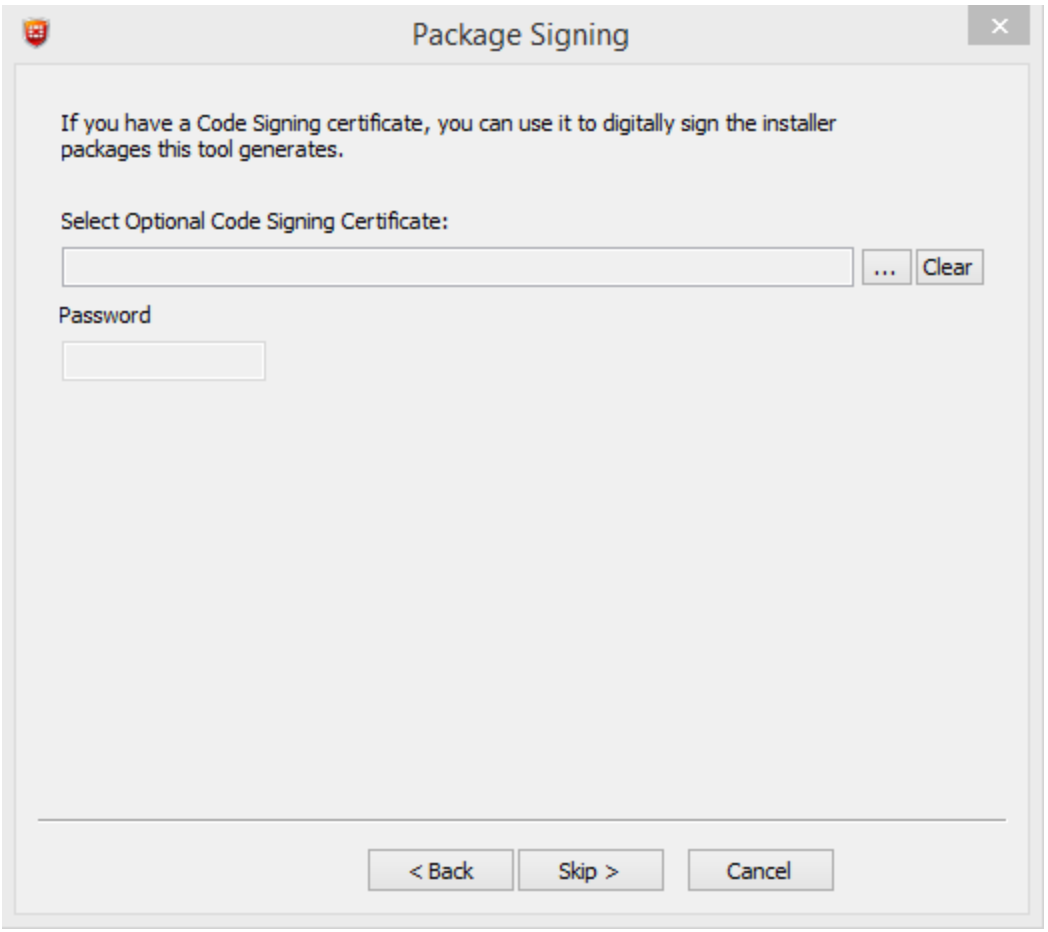
About_red_shield_logo.png	Where Used: File Type: PNG File (.png) Width: 43 pixels Height: 43 pixels Bit Depth: 32
Advertisement_ad_0.png	Where Used: Dashboard advertisement banner File Type: PNG File (.png) Width: 628 pixels Height: 66 pixels Bit Depth: 32

Advertisement_ad_1.png	Where Used: Dashboard advertisement banner File Type: PNG File (.png) Width: 628 pixels Height: 66 pixels BitBit Depth: 32
Advertisement_ad_2.png	Where Used: Dashboard advertisement banner File Type: PNG File (.png) Width: 628 pixels Height: 66 pixels Bit Depth: 32
Antivirus_AV_scan_top_banner_left_hand_side.png	Where Used: File Type: BMP File (.bmp) Width: 1 pixel Height: 40 pixels Bit Depth: 8
Antivirus_AV_scan_top_banner_right_hand_side.png	Where Used: Banner used in right-click “scan with product name” dialog box File Type: BMP File (.bmp) Width: 440 pixels Height: 40 pixels Bit Depth: 8
Common_fgt-not-found-page-bg.png	Where Used: FortiGate not found page File Type: PNG File (.png) Width: 673 pixels Height: 189 pixels Bit Depth: 32
Common_fortinet-icon.png	Where Used: File Type: PNG File (.png) Width: 79 pixels Height: 79 pixels Bit Depth: 32
Common_registration_icon.png	Where Used: FortiGate detected page File Type: PNG File (.png) Width: 85 pixels Height: 85 pixels Bit Depth: 32
Common_searching-page-bg.png	Where Used: Searching for FortiGate page File Type: PNG File (.png) Width: 673 pixels Height: 189 pixels Bit Depth: 32

Dashboard_forticlient_v5_dashboard_bg.png	Where Used: Client console File Type: PNG File (.png) Width: 628 pixels Height: 451 pixels Bit Depth: 32
Dashboard_warning-shield.png	Where Used: Dashboard warning shield, displayed when antivirus is disabled. File Type: PNG File (.png) Width: 59 pixels Height: 75 pixels Bit Depth: 32
Installer_background.bmp	Where used: Setup Wizard background image. File Type: BMP file (.bmp) Width: 491 pixels Height: 312 pixels Bit Depth: 8
Installer_banner.bmp	Where Used: Setup Wizard banner image on destination page, ready to install page, installing pages. File Type: BMP file (.bmp) Width: 491 pixels Height: 58 pixels Bit Depth: 8
LightInstaller_icon.ico	Where Used: Light Installer Icon File Type: ICO File (.ico) Width: 32 pixels Height: 32 pixels Bit Depth: 32
Main_icon.ico	Where Used: Shortcut on desktop File Type: ICO file (.ico) Width: 48 pixels Height: 48 pixels Bit Depth: 32
Main_logo_black.ico	Where Used: Client console header File Type: ICO file (.ico) Width: 32 pixels Height: 32 pixels Bit Depth: 32
setup.ico	Where Used: Setup icon File Type: ICO File (.ico) Width: 256 pixels Height: 256 pixels Bit Depth: 32

Tray_Icons_alert.ico	Where Used: System tray alert icon File Type: ICO File (.ico) Width: 16 pixels Height: 16 pixels Bit Depth: 32
Tray_Icons_alert_vpn.ico	Where Used: System tray VPN alert icon File Type: ICO File (.ico) Width: 16 pixels Height: 16 pixels Bit Depth: 32
Tray_Icons_running.ico	Where Used: System tray running icon File Type: ICO File (.ico) Width: 16 pixels Height: 16 pixels Bit Depth: 32
Tray_Icons_scan1.ico, Tray_Icons_scan2.ico, Tray_Icons_scan3.ico, Tray_Icons_scan4.ico, Tray_Icons_scan5.ico, Tray_Icons_scan6.ico, Tray_Icons_scan7.ico, Tray_Icons_scan8.ico, Tray_Icons_scan9.ico, Tray_Icons_scan10.ico Tray_Icons_scan11.ico	Where Used: System tray, these eleven images animate the scanning activity of the tray icon. File Type: ICO File (.ico) Width: 16 pixels Height: 16 pixels Bit Depth: 32
Tray_Icons_vpn.ico	Where Used: System tray VPN icon File Type: ICO File (.ico) Width: 16 pixels Height: 16 pixels Bit Depth: 32
VPN_xauth-dialog-logo.png	Where Used: VPN xAuth dialog logo File Type: PNG File (.png) Width: 88 pixels Height: 100 pixels Bit Depth: 32
zzz_rebranding.ini	Where Used: This file is used by the FortiClient Configurator tool for element/resource mapping. File Type: Configuration settings (.ini)

When rebranding FortiClient, you can select to digitally sign the installer package using a code signing certificate.


Package Signing
If you have a Code Signing certificate, you can use it to digitally sign the installer packages this tool generates.
Select Optional Code Signing Certificate:
...
Clear
Password
< Back
Skip >
Cancel

Appendix D - FortiClient Log Messages

Client Feature	ID	Level	Format	Description
Antivirus	0x00017912	Warning	Found virus by [Antivirus scan|Antivirus realtime protection] in [filesystem|disk|email]	This message is logged when a virus is found.
Antivirus	0x00017913	Warning	Found malware by [Antivirus scan|Antivirus realtime protection] in [filesystem|email]	This message is logged when a malware is found.
Antivirus	0x00017914	Warning	Found suspicious by [Antivirus scan|Antivirus realtime protection] in [filesystem|disk|email]	This message is logged when a suspicious is found.
Antivirus	0x00017915	Info	User enabled Realtime Antivirus protection	Logged when someone enables Realtime Antivirus.
Antivirus	0x00017916	Warning	User disabled Realtime Antivirus protection	Logged when someone disables Realtime Antivirus.
Antivirus	0x00017917	Info	Communication error, [detailed info], err=[error_code]	Communication error with other modules
Antivirus	0x00017918	Warning	Antivirus realtime protection killed malware process : [process name]	A malware process killed a malware process.
Antivirus	0x0001791d	Info	av_task scan is started	This message is logged if AV scanning is started.
Antivirus	0x0001791e	Info	av_task scan is stopped	This message is logged if AV scanning is stopped.
Antivirus	0x00017919	Info	av_task scan thread is suspended	This message is logged if AV scanning is paused.
Antivirus	0x0001791a	Info	av_task scan thread is resumed	This message when AV scanning is resumed.
Antivirus	0x0001791b	Warning	av_task killed suspicious process : <filename or process name>	<filename or process name> is a suspicous process and has been terminated.

Client Feature	ID	Level	Format	Description
Antivirus	0x0001791c	Info	Cannot start scan task, license expired	License expired.
Antivirus	0x0001791f	Error	Scheduled scan failed: Path to file/folder no longer exists.	Path not found.
Webfilter	0x000178f4	Info	User enabled Webfilter	Logged when someone enables webfiltering.
Webfilter	0x000178f5	Warning	User disabled Webfilter	Logged when someone disables webfiltering.
Webfilter	0x000178f6	Warning	user's access to the url [action and reason]	the action to the user's access, and the reason
Webfilter	0x000178f7	Info	user's access to the url [action and reason]	the action to the user's access, and the reason
Webfilter	0x000178f8	Warning	The Webfilter Violation report was cleared [user name]	Logged when someone clears the webfilter violation report.
Webfilter	0x000178f9	Warning	Unable to create proxy/webfilter communication socket.	FortiClient will not be able to determine the FortiGuard rating of URLs.
Webfilter	0x000178fa	Warning	Unable to retrieve the webfilter UDP port number.	FortiClient will not be able to determine the FortiGuard rating of URLs.
Webfilter	0x000178fb	Warning	status=warn [logged on user] temporarily disabled blocking of category [category id] ([category name]) to access [url]	The user [logged on user] proceeded to the url [url] after acknowwledging a warning message.
Application FireWall	0x00017980	Warning	Firewall action, type=[num] protocol=[num] direction=[num] source=[addr] destination= [addr]	Firewall action
Application FireWall	0x00017981	Info	Firewall action, type=[num] protocol=[num] direction=[num] source=[addr] destination= [addr]	Firewall action
Application FireWall	0x00017982	Info	User enabled Firewall	User enabled Firewall

Client Feature	ID	Level	Format	Description
Application FireWall	0x00017983	Warning	User disabled Firewall	User disabled Firewall
Application FireWall	0x00017984	Warning	The Application Firewall report was cleared	Logged when someone clears the application firewall report.
IKE VPN	0x00017930	Info	VPN tunnel status	VPN tunnel status
IKE VPN	0x00017931	Warning	locip=<ip address> locport=<port number> remip=<ip address> remport=<port number> outif=<interface> vpntunnel=<tunnel name> status=negotiate_error msgg=No response from the peer, phase1 retransmit reaches maximum count.	No response from the peer, phase1 retransmit reaches maximum count.
IKE VPN	0x00017932	Warning	locip=<ip address> locport=<port number> remip=<ip address> remport=<port number> outif=<interface> vpntunnel=<tunnel name> status=negotiate_error msgg=No response from the peer, phase2 retransmit reaches maximum count.	No response from the peer, phase2 retransmit reaches maximum count.
IKE VPN	0x00017933	Warning	locip=<ip address> locport=<port number> remip=<ip address> remport=<port number> outif=<interface> vpntunnel=<tunnel name> status=negotiate_error msgg=Received delete payload from peer check xauth password.	Received delete payload from peer check xauth password.
IKE VPN	0x00017934	Error	locip=<ip address> locport=<port number> remip=<ip address> remport=<port number> outif=<interface> vpntunnel=<tunnel name> msg=Failed to acquire an IP address.	Failed to acquire an IP address for the virtual adapter.
IKE VPN	0x00017935	Error	ike error, <detailed error info>	General error of IKE

Client Feature	ID	Level	Format	Description
IKE VPN	0x00017936	Info	negotionation information, <detailed info>	negotionation information
IKE VPN	0x00017937	Error	negotionation error, <detailed error>	negotionation error
IKE VPN	0x00017938	Error	replayed packet detected (packet dropped), <detailed error>	replayed packet detected (packet dropped).
IKE VPN	0x00017939	Info	VPN user accept the banner and continue with the tunnel setup	The VPN user accept the banner warning
IKE VPN	0x0001793a	Info	VPN user choose disconnect the tunnel or no response	The VPN user reject the banner warning and disconnect the tunnel
IKE VPN	0x0001793b	Info	locip=<ip address> locport=<port number> remip=<ip address> remport=<port number> outif=<interface> vpntunnel=<tunnel name> action=install_sa, inspi=<inbound spi> outspi=<outbound spi> <Initiator|Responder> tunnel <ip address/ip address> install sa	Send sa to the IPsec driver.
IKE VPN	0x0001793c	Info	VPN before logon was enabled	Logged when someone enables VPN before logon.
IKE VPN	0x0001793d	Info	VPN before logon was disabled	Logged when someone disables VPN before logon.
SSL VPN	0x00017958	Info	SSLVPN tunnel status	SSLVPN tunnel status
Wan Acceleration	0x00017a71	Info	User enabled WAN Acceleration	User enabled WAN Acceleration
Wan Acceleration	0x00017a70	Info	User disabled WAN Acceleration	User disabled WAN Acceleration

Client Feature	ID	Level	Format	Description
Wan Acceleration	0x0000b000	Error	Network registry keys are missing	When enumerating the network interface subkeys, it was found that there were no subkeys present.
Wan Acceleration	0x0000b001	Error	Network adapter is missing a description	When enumerating the network interfaces, one was found without a descriptions.
Wan Acceleration	0x0000b002	Error	Error opening redirector device	Wan acceleration will not function.
Wan Acceleration	0x0000b003	Info	WAN Acceleration was enabled by [user name]	Logged when someone enables WAN Acceleration.
Wan Acceleration	0x0000b004	Info	WAN Acceleration was disabled by [user name]	Logged when someone disables WAN Acceleration.
Vulnerability Scan	0x00017908	Info	The vulnerability scan status has changed	A vulnerability scan status change
Vulnerability Scan	0x00017909	Info	A vulnerability scan result has been logged	A Vulnerability scan result log
EndPoint Control	0x00017ab6	Info	upload logs, [state]	Upload logs to registered FortiGate
EndPoint Control	0x00017ab7	Info	Endpoint control policy synchronization was enabled	Logged when someone enables Endpoint control policy synchronization.
EndPoint Control	0x00017ab8	Warning	Endpoint control policy synchronization was disabled	Logged when someone disables Endpoint control policy synchronization.
EndPoint Control	0x00017ab9	Info	Endpoint Control Status changed to [status]	Endpoint Control Status Changed
EndPoint Control	0x00017aba	Warning	OffNet configuration version [version] doesn't match FortiGate configuration version [version]	OffNet configuration version doesn't match FortiGate configuration version
EndPoint Control	0x00017abb	Info	Endpoint Control Registration Status changed to [status] with FGT [serial], [address] and client ip [address]	Endpoint Control Registration Status Changed

Client Feature	ID	Level	Format	Description
Update	0x00017a2a	Info	Customer initiated a software update request.	Logged when a user presses the gui's update button.
Update	0x00017a37	Info	Checking for updates.	Checking for updates.
Update	0x00017a2c	Info	Update allowed only if you have a valid license	Update allowed only if you have a valid license
Update	0x00017a38	Info	Software update started.	Software update started.
Update	0x00017a2d	Info	Software updates are disabled.	Software updates from FortiGuard have been disabled.
Update	0x00017a2e	Info	Software updates from from FortiGuard have been disabled becaue this client is managed.	Software updates from FortiGuard have been disabled.
Update	0x00017a2f	Info	Software updates require administrative privileges.	The user does not have sufficient priviledges to perform software updates.
Update	0x00017a30	Info	Software update successful.	Software update successful.
Update	0x00017a31	Info	Software update failed.	Software update failed.
Update	0x00017a32	Info	Unable to perform software update. Registry does not contain image id to download.	The image id that is expected to be in the registry is missing.
Update	0x00017a33	Info	Update <module description> successful, new version is <version number>	Update was successful to the given version for the given module.
Update	0x00017a34	Error	Unable to load AV engine	Failed to load the av engine
Update	0x00017a35	Error	Error patching AV signature.	Error patching AV signature.
Update	0x00017a36	Error	Unable to load FASLE engine	Unable to load FASLE engine
Update	0x00017a39	Info	Update successful, <all engine/signature versions>	Update was successful, current engine/signature information recorded.

Client Feature	ID	Level	Format	Description
Scheduler	0x00017a20	Info	Forcefully kill a child process after grace period expires	A scheduler owned child process failed to stop when instructed to do so, so was forcefully terminated.
Scheduler	0x00017a21	Error	The scheduler cannot start the scheduled task because the task's license is expired.	The scheduler cannot start the scheduled task because the task's license is expired.
Scheduler	0x00017a68	Info	FortiClient is starting up	FortiClient is starting up
Scheduler	0x00017a69	Info	%s is shutting down	FortiClient is shutting down
FortiProxy	0x00017a49	Info	Fortiproxy is enabled	Fortiproxy is enabled
FortiProxy	0x00017a48	Warning	Fortiproxy is disabled	Fortiproxy is disabled
FortiShield	0x00017a53	Info	FortiShield is enabled	FortiShield is enabled
FortiShield	0x00017a52	Warning	FortiShield is disabled	FortiShield is disabled
FortiShield	0x00017a54	Info	The console was locked	The console password was locked.
FortiShield	0x00017a55	Warning	The console was unlocked	The console password was unlocked.
FortiShield	0x00017a56	Warning	The console password was removed	The console password was removed.
FortiShield	0x00017a57	Warning	FortiShield blocked application: [application path] from modifying: [file or registry path]	FortiShield has prevented an application from modifying a file or registry setting protected by FortiClient.
Application Database	0x0000d001	Error	<context> <file reference> db error - creating new database.	A critical error occured. The application database will not work. <context> is the service that generated the log. <file reference> is optional and describes the file was being accessed when the log was generated.

Client Feature	ID	Level	Format	Description
Application Database	0x0000d003	Error	<context> <file reference> db error - BIND command.	A critical error occured. The application database will not work. <context> is the service that generated the log. <file reference> is optional and describes the file was being accessed when the log was generated.
Application Database	0x0000d004	Error	<context> <file reference> db error - opening database.	A critical error occured. The application database is not present. An attempt to automatically regenerate it will occur. <context> is the service that generated the log. <file reference> is optional and describes the file was being accessed when the log was generated.
Application Database	0x0000d005	Error	<context> <file reference> db error - preparing sql statement.	The sql statement used is invalid. <context> is the service that generated the log. <file reference> is optional and describes the file was being accessed when the log was generated.
Application Database	0x0000d006	Error	<context> <file reference> db error - unable to find fingerprint.	The fingerprint does not exist in the database. <context> is the service that generated the log. <file reference> is optional and describes the file was being accessed when the log was generated.
Application Database	0x0000d007	Error	<context> <file reference> db error - invalid md5.	The parameter supplied is not an MD5. <context> is the service that generated the log. <file reference> is optional and describes the file was being accessed when the log was generated.

Client Feature	ID	Level	Format	Description
Application Database	0x0000d008	Error	<context> <file reference> db error - row not found.	The requested row does not exist. <context> is the service that generated the log. <file reference> is optional and describes the file was being accessed when the log was generated.
Application Database	0x0000d00a	Error	<context> <file reference> Can't open file.	The file cannot be opened. <context> is the service that generated the log. <file reference> is optional and describes the file was being accessed when the log was generated.
Application Database	0x0000d00b	Error	<context> <file reference> Unable to extract vendor id.	The files is not digitally signed, or the signature cannot be read. <context> is the service that generated the log. <file reference> is optional and describes the file was being accessed when the log was generated.
Application Database	0x0000d00e	Error	<context> <file reference> Can't access file because of sharing violation.	Can't access file because of sharing violation. <context> is the service that generated the log. <file reference> is optional and describes the file was being accessed when the log was generated.
Application Database	0x0000d00f	Error	<context> <file reference> Can't open driver.	Can't open the apd driver. <context> is the service that generated the log. <file reference> is optional and describes the file was being accessed when the log was generated.
Application Database	0x0000d010	Error	<context> <file reference> Can't start driver.	Can't start the apd driver. <context> is the service that generated the log. <file reference> is optional and describes the file was being accessed when the log was generated.

Client Feature	ID	Level	Format	Description
Application Database	0x0000d011	Error	<context> <file reference> Driver io error.	APD driver io error. <context> is the service that generated the log. <file reference> is optional and describes the file was being accessed when the log was generated.
Application Database	0x0000d016	Error	<context> <file reference> Server-side pipe error.	A communication error occured. It is probably temporary. <context> is the service that generated the log. <file reference> is optional and describes the file was being accessed when the log was generated.
Application Database	0x0000d017	Error	<context> <file reference> Pipe server initialization error.	A communication initializion error occured. It is probably temporary. <context> is the service that generated the log. <file reference> is optional and describes the file was being accessed when the log was generated.
Application Database	0x0000d018	Error	<context> <file reference> Pipe server creation error.	A communication initializion error occured. It is probably temporary. <context> is the service that generated the log. <file reference> is optional and describes the file was being accessed when the log was generated.
Application Database	0x0000d019	Error	<context> <file reference> Unable to bypass fortishield.	Failed to bypass self-protection. The daemon might not function normally after this. <context> is the service that generated the log. <file reference> is optional and describes the file was being accessed when the log was generated.

Client Feature	ID	Level	Format	Description
Application Database	0x0000d01a	Error	<context> <file reference> Invalid arguments.	Invalid command line options supplied. <context> is the service that generated the log. <file reference> is optional and describes the file was being accessed when the log was generated.
Application Database	0x0000d01c	Error	<context> <file reference> Unable to allocate memory for vendor id cache.	Low memory. <context> is the service that generated the log. <file reference> is optional and describes the file was being accessed when the log was generated.
Application Database	0x0000d01d	Error	<context> <file reference> Vendor id cache not initialized.	This is probably temporary. An attempt will be made later to read/write to the cache. <context> is the service that generated the log. <file reference> is optional and describes the file was being accessed when the log was generated.
Application Database	0x0000d01e	Error	<context> <file reference> Unable to open vendor id cache shared memory.	Application detection will not be functioning normally. <context> is the service that generated the log. <file reference> is optional and describes the file was being accessed when the log was generated.
Application Database	0x0000d01f	Error	<context> <file reference> Unable to open mutex to access vendor id shared memory.	Application detection will not be functioning normally. <context> is the service that generated the log. <file reference> is optional and describes the file was being accessed when the log was generated.
Config Import/Export	0x00017a5c	Info	A configuration file is exported to [location]	Logged when someone exports a config file.
Config Import/Export	0x00017a5d	Info	A configuration file is imported from [location]	Logged when someone imports a config file.

Client Feature	ID	Level	Format	Description
Single Sign-On Mobility Agent	0x00017ad4	Info	Single Sign-On event	Single Sign-On event.
Single Sign-On Mobility Agent	0x00017ad5	Info	Single Sign-On Mobility Agent was enabled	Logged when someone enables Single Sign-On Mobility Agent.
Single Sign-On Mobility Agent	0x00017ad6	Warning	Single Sign-On Mobility Agent was disabled	Logged when someone disables Single Sign-On Mobility Agent.
Single Sign-On Mobility Agent	0x00017ad7	Info	Single Sign-On Mobility Agent is starting..., version:[nnn]	Single Sign-On Mobility Agent is starting
Single Sign-On Mobility Agent	0x00017ad8	Info	Single Sign-On Mobility Agent is stopping..., version:[nnn]	Single Sign-On Mobility Agent is stopping
UI	0x00017a66	Warning	Logs were cleared	Logged when logs are cleared.
UI	0x00017a67	Info	Alerts were cleared	Logged when alerts are cleared by a user.